BOGOTÁ MI CIUDAD MI CASA

BOGOTÁ

# ALCALDÍA MAYOR DE BOGOTÁ D.C.
# SECRETARÍA GENERAL

## ESTRATEGIA PARA LA GESTIÓN DE RIESGOS
# EN EL MARCO DE LOS PROGRAMAS
# DE TRANSPARENCIA Y ÉTICA PÚBLICA

Orientaciones para la implementación del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, en las entidades distritales

**Bogotá D.C.**
**2026**



Dirección Distrital de Desarrollo Institucional
Subsecretaría Distrital de Fortalecimiento Institucional
Secretaría General de la Alcaldía Mayor de Bogotá D.C.

# ALCALDÍA MAYOR DE BOGOTÁ D.C.

## Secretaría General de la Alcaldía Mayor de Bogotá

**Carlos Fernando Galán Pachón**
*Alcalde Mayor de Bogotá D.C.*

**Miguel Andrés Silva Moyano**
*Secretario General de la Alcaldía Mayor de Bogotá*

**Alejandra Rodas Gaiter**
*Subsecretaria Distrital de Fortalecimiento Institucional*

**Juan Camilo Giraldo Zuluaga**
*Director Distrital de Desarrollo Institucional*

**Oscar Orlando Simmonds Pachón**
*Subdirector Técnico para la Generación de Capacidades Institucionales*

## Equipo Técnico

**Linda Mirielly Joanne Reales Magdaniel**

**Derli Yarley Portillo Salguero**

**Katerin Lorena Cardozo Palacios**

**Karyn Estefanía Sáenz Barrera**

**David Ricardo Fiscó Lombo**

**Luz Antonia Martínez Ruíz**

**Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP**

**Octubre de 2026**

**Transparencia en el uso de IA: En coherencia con los principios de transparencia, responsabilidad y trazabilidad, este documento integra aportes derivados del análisis humano experto y del uso asistido de herramientas de inteligencia artificial generativa para la corrección de estilo. Su contenido fue verificado por el equipo técnico institucional antes de su aprobación.**

INTRODUCCIÓN ..... 5
Objetivo ..... 7
Alcance ..... 8
Marco conceptual ..... 8
Siglas y Abreviaturas ..... 14
¿Qué es el SIGRIP? ..... 16
¿Cómo se articula el SIGRIP con el PTEP? ..... 17
¿Cómo se articula el SIGRIP con MIPG y MECI? ..... 17
Capítulo 1 Gestión del Riesgo para las Amenazas de Fraude, Soborno, Corrupción e Inadecuada Gestión del Conflicto de Interés ..... 18
1.1 Gestión del riesgo de las amenazas de Fraude Interno, Soborno y Corrupción. ..... 18
1.1.1. Contexto del componente. ..... 18
1.1.2 Políticas Antisoborno y Antifraude ..... 21
Declaración de compromisos Política de Riesgos Antisoborno ..... 22
Declaración de compromiso Política de Riesgos Antifraude ..... 22
Los servidores deberán: ..... 22
Los servidores se abstendrán de: ..... 23
1.2. Conflicto de interés ..... 24
1.2.1 Recomendaciones para la elaboración de un procedimiento para la adecuada gestión de conflictos de interés ..... **¡Error! Marcador no definido.**
Capítulo 2 Gestión del Riesgo de Lavado de activos (LA), financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) ..... 33
2.1. Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva (ALA/CFT/CFP) ..... 35
2.1.1. Declaración de la Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva (ALA/CFT/CFP) ..... 36
2.2. ¿Cómo diferenciar las amenazas LA/FT/FP en la gestión institucional? ..... 39
2.3. El LA/FT/FP como amenaza a la Integridad Pública ..... 40
2.4. Articulación con los demás elementos del SIGRIP. ..... 46
2.5. Procedimiento para el Reporte de Operaciones Sospechosas ..... 47
2.5.1. Contexto Normativo y alcance del componente ..... 47

2.5.2. ¿Qué se espera del componente en el SIGRIP Distrital? ..... 48
Capítulo 3 Función de Cumplimiento ..... 59
3.1. Contexto Normativo y alcance transversal ..... 59
3.2. ¿Qué es la función de cumplimiento y por qué es relevante para las entidades distritales? ..... 61
3.3. ¿Qué se espera del componente en el SIGRIP Distrital? ..... 61
3.4. Asignación y condiciones del ejercicio de la función. ..... 63
Capítulo 4 Debida diligencia en el conocimiento de las contrapartes ..... 64
4.1. Contexto y alcance del componente. ..... 64
4.4. Implementación del componente de Debida Diligencia ..... 70
4.5. Construcción del Manual de Debida Diligencia ..... 73
Capítulo 5 Canales de Denuncia ..... 75
5.1. Contexto normativo y conceptual ..... 75
5.1.2 Elementos para la gestión de denuncias ..... 76
5.2. Recomendaciones para la elaboración del procedimiento para la operación del canal institucional de denuncias por corrupción. ..... 77
Bibliografía ..... 79

# Introducción

La integridad pública constituye una condición esencial para el cumplimiento de los fines del Estado, la protección del interés general y la generación de confianza entre las instituciones y la ciudadanía. Su fortalecimiento requiere que las entidades públicas desarrollen capacidades para identificar, prevenir, detectar y gestionar oportunamente aquellas situaciones que puedan afectar la transparencia, la legalidad, la adecuada administración de los recursos públicos y el cumplimiento de sus objetivos institucionales.

En este marco, la Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7, expedida en 2025 por el Departamento Administrativo de la Función Pública (DAFP), en articulación con la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones, actualizó el enfoque para la gestión de los riesgos que afectan la integridad pública e incorporó el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP). Este sistema aborda integralmente cinco amenazas contra la integridad pública: la corrupción, el fraude, el soborno, la inadecuada gestión de los conflictos de interés y la amenaza asociada al lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva (LA/FT/FPADM).

En el ámbito nacional, la gestión de los riesgos para la integridad pública se desarrolla en el marco de los Programas de Transparencia y Ética Pública (PTEP), previstos en el artículo 31 de la Ley 2195 de 2022 y reglamentados mediante el Decreto 1122 de 2024. Si bien la gestión de riesgos debe abordarse de manera integral y articulada frente al conjunto de riesgos que pueden afectar el cumplimiento de los objetivos de una entidad pública, aquellos que pueden comprometer la integridad pública requieren una atención específica, dada su incidencia en la transparencia, la confianza institucional y la prevención de prácticas contrarias al interés general. Por esta razón, su gestión se incorpora de manera expresa en los PTEP, cuyo componente programático incluye el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), como estrategia institucional para prevenir y gestionar las amenazas que pueden afectar la integridad pública. Sobre esta base, la presente Estrategia orienta y fortalece la aplicación del SIGRIP en las entidades y organismos del Distrito Capital, considerando sus características, capacidades institucionales y obligaciones aplicables.

Adicionalmente, algunas entidades y empresas del Distrito pueden encontrarse sujetas a la obligación de adoptar Programas de Transparencia y Ética Empresarial (PTEE), de acuerdo con su naturaleza jurídica, el sector en el que operan y las disposiciones expedidas por la respectiva autoridad de inspección, vigilancia o control. Esta particularidad resulta relevante para la aplicación de la Estrategia, especialmente porque el Decreto 1122 de 2024 contempla reglas específicas para las entidades obligadas al PTEP que operen en mercados, industrias o sectores en los que la autoridad competente exija un PTEE. En estos casos, las entidades deberán atender el régimen que les resulte aplicable y armonizar sus instrumentos de gestión cuando corresponda, evitando duplicidades y cargas innecesarias.

En este contexto, la Secretaría General de la Alcaldía Mayor de Bogotá, en ejercicio de sus funciones de orientación y fortalecimiento institucional en materia de transparencia, integridad y

prevención de la corrupción, presenta la Estrategia para la Gestión de Riesgos del SIGRIP, dirigida a orientar su aplicación en las entidades y organismos distritales. Su denominación como Estrategia responde a que el documento, además de proporcionar orientaciones técnicas, propone una ruta para abordar los diferentes elementos del SIGRIP y fortalecer progresivamente su gestión, teniendo en cuenta las características y capacidades institucionales de cada entidad.

En consecuencia, la Estrategia no supone la creación de un sistema completamente nuevo ni parte de la premisa de que las entidades deban implementar desde cero mecanismos para gestionar estas amenazas. Por el contrario, reconoce las capacidades institucionales existentes y busca proporcionar un marco común para articular, alinear y fortalecer los instrumentos, metodologías, controles y mecanismos que ya se encuentran en operación, identificar brechas y orientar su evolución progresiva de acuerdo con el contexto, la exposición al riesgo, las obligaciones aplicables y el nivel de desarrollo institucional de cada entidad. Bajo esta lógica, las orientaciones técnicas contenidas en el documento constituyen instrumentos para desarrollar la Estrategia, pero no agotan su alcance.

Esta articulación resulta necesaria porque las amenazas contra la integridad pública no se presentan de manera aislada. La corrupción, el fraude, el soborno, la inadecuada gestión de los conflictos de interés y el LA/FT/FP pueden compartir factores de riesgo, vulnerabilidades, controles y consecuencias institucionales. Una gestión fragmentada puede generar duplicidades, vacíos, responsabilidades dispersas o controles desarticulados. Frente a ello, la Estrategia proporciona un lenguaje común, criterios técnicos y herramientas que favorecen una gestión integral, coherente, eficiente y verificable, al tiempo que permiten reconocer las particularidades y capacidades de cada entidad.

La Estrategia se articula con los principios, políticas e instrumentos del Modelo Integrado de Planeación y Gestión (MIPG) y con el Modelo Estándar de Control Interno (MECI), de manera que la gestión de los riesgos para la integridad pública se integre a la gestión institucional y no se desarrolle como un ejercicio aislado o exclusivamente documental. En particular, el esquema de líneas de defensa permite delimitar las responsabilidades relacionadas con la gestión, supervisión, seguimiento y evaluación de los riesgos y controles. Esta articulación favorece la incorporación del SIGRIP en los procesos y mecanismos de gestión existentes en las entidades, evitando que se convierta en una carga adicional o desconectada de su operación.

La aplicación de la Estrategia se sustenta, además, en un enfoque basado en riesgo y en criterios de proporcionalidad. Esto implica que las medidas, controles y mecanismos de fortalecimiento deben responder a las características y al contexto de cada entidad, sus procesos, las contrapartes con las que se relaciona, su exposición a las diferentes amenazas contra la integridad pública y las obligaciones que le resulten aplicables. En consecuencia, la Estrategia no pretende imponer idénticas medidas a todas las entidades, sino orientar la priorización de esfuerzos y recursos en función de sus riesgos, necesidades y capacidades institucionales.

Para facilitar su aplicación, el documento desarrolla orientaciones técnicas relacionadas con la gestión de riesgos frente a las amenazas de fraude, soborno, corrupción, inadecuada gestión de los conflictos de interés, LA/FT/FP; la función de cumplimiento; la debida diligencia en el conocimiento de contrapartes; y los canales institucionales de denuncia. Asimismo, incorpora herramientas metodológicas, ejemplos orientadores de instrumentos institucionales, un mecanismo de autodiagnóstico y un modelo de madurez que permiten a cada entidad reconocer

sus capacidades, identificar brechas y definir acciones de fortalecimiento acordes con su contexto y nivel de desarrollo institucional.

Uno de los principios que orienta la Estrategia es la progresividad en el fortalecimiento de las capacidades institucionales. En consecuencia, el modelo de madurez permite reconocer diferentes niveles de desarrollo y orientar el avance de las entidades a partir de tres niveles: Inicial, Definido y Optimizado. El nivel Inicial se concentra en las condiciones básicas y en el cumplimiento de los requerimientos normativos aplicables; el nivel Definido supone una mayor formalización, articulación e integración de los componentes del SIGRIP con los procesos y mecanismos de gestión institucional; y el nivel Optimizado refleja capacidades consolidadas e incorpora buenas prácticas y referentes técnicos nacionales e internacionales que permiten profundizar la gestión preventiva del riesgo. Los estándares y referentes internacionales incorporados en este último nivel tienen carácter orientador cuando no constituyan obligaciones directamente aplicables a la entidad.

El autodiagnóstico constituye el punto de partida para determinar las capacidades institucionales existentes y orientar esta ruta de fortalecimiento. A través de este instrumento, cada entidad puede establecer su nivel de madurez en los diferentes componentes, identificar brechas y priorizar las acciones requeridas para avanzar progresivamente. Por esta razón, el desarrollo institucional no necesariamente será uniforme entre todos los componentes del SIGRIP. Una entidad puede contar con capacidades más avanzadas en algunos ámbitos y requerir mayores esfuerzos de fortalecimiento en otros.

Las orientaciones y herramientas contenidas en esta Estrategia deberán aplicarse de acuerdo con el marco jurídico que corresponda a cada entidad. En consecuencia, no sustituyen ni modifican las obligaciones legales, reglamentarias o sectoriales aplicables, particularmente aquellas derivadas de la naturaleza jurídica de la entidad, su actividad o su régimen de inspección, vigilancia y control. Los referentes técnicos y las buenas prácticas que excedan las obligaciones vigentes se incorporan como mecanismos de fortalecimiento progresivo y deberán ser valorados de acuerdo con el nivel de madurez, la exposición al riesgo y las capacidades de cada entidad.

Más que un ejercicio de cumplimiento normativo, esta Estrategia busca constituirse en una herramienta práctica para el fortalecimiento institucional y para la consolidación de una cultura basada en la integridad, la transparencia y la gestión preventiva del riesgo. El cumplimiento de las obligaciones aplicables constituye el punto de partida, no la finalidad última de la Estrategia. Su propósito es contribuir al desarrollo de capacidades que permitan anticipar riesgos, fortalecer los controles, mejorar la toma de decisiones, proteger la confianza pública y generar valor público para la ciudadanía.

# Objetivo

Orientar a las entidades del Distrito en la implementación del Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP, base del componente programático - Estrategia Institucional para la Lucha Contra la Corrupción en el marco del Programa de Transparencia y Ética Pública, con el propósito de contribuir a la gestión adecuada de los riesgos para la integridad pública.

# Alcance

La presente Estrategia orienta la gestión de los riesgos para la integridad pública en las entidades y organismos del Distrito Capital obligados a implementar Programas de Transparencia y Ética Pública, mediante la articulación e incorporación del SIGRIP en sus procesos institucionales. Comprende la gestión de los riesgos asociados a las amenazas de corrupción, soborno, fraude, inadecuada gestión de los conflictos de interés y lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva (LA/FT/FP), así como la aplicación de medidas de debida diligencia, los canales de denuncia, la función de cumplimiento y las demás herramientas que hacen parte del Sistema.

El SIGRIP se implementa de manera articulada con el PTEP, el MIPG, el MECI y los demás instrumentos institucionales de gestión y control que resulten aplicables, procurando aprovechar las estructuras, metodologías y capacidades existentes y evitar la generación de esquemas paralelos o duplicidades.

Para las entidades y empresas distritales sujetas a Programas de Transparencia y Ética Empresarial o a otros sistemas sectoriales de gestión de riesgos, las orientaciones de la Estrategia se aplicarán de manera armónica y complementaria con el régimen especial correspondiente, de acuerdo con su naturaleza jurídica y las obligaciones que les resulten aplicables, evitando duplicidades.

# Marco conceptual

**Causales de impedimento:** son las situaciones definidas por la ley que comprometen la objetividad e imparcialidad de un servidor público, obligándolo a apartarse del conocimiento de un asunto específico. (Artículo 11 de la ley 1437 de 2011)

**Círculos de afinidad y consanguinidad:** Son las relaciones de parentesco que la ley reconoce entre personas, relevantes para determinar posibles conflictos de interés e impedimentos. (Artículo 11 de la ley 1437 de 2011)

- **Afinidad:** vínculo que surge por matrimonio o unión permanente con los parientes del cónyuge o compañero permanente.
- **Consanguinidad:** vínculo entre personas que descienden de un mismo tronco familiar (padres, hijos, hermanos, primos, etc.).

**Colaborador:** persona que contribuye al cumplimiento de los objetivos y fines institucionales de la entidad, independientemente de la naturaleza de su vinculación. Para efectos la presente estrategia, el término comprende a los servidores públicos, trabajadores oficiales, contratistas y demás personas que desarrollen actividades en favor de la entidad[1].

[1] El Departamento Administrativo del Servicio Civil Distrital indicó que el término "colaborador" puede emplearse para referirse a todas las personas que prestan sus servicios en las entidades y organismos, independientemente de su forma de vinculación, comprendiendo empleados públicos, trabajadores oficiales y contratistas. (Concepto 2021EE956. Respuesta al radicado 2021ER728 sobre la utilización del término colaboradores en la administración pública, 2021)

**Conflicto de interés:** se presenta cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público. El interés del servidor público se presenta cuando debe decidir sobre asuntos en los que tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. (A partir de la Ley 1952 de 2019, art. 44, Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011). (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

**Contraparte:** cualquier persona o entidad que tenga un interés propio o particular, diferente al interés de la organización. (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

**Corrupción:** todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral. (A partir del artículo 2.1.4.3.1.3 del Decreto 1081 de 2015). (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

**Denuncia:** reporte, comunicación o informe sobre un hecho irregular, que puede ser generado por cualquier persona con el fin de que la autoridad competente investigue y sancione una posible conducta reprochable o contraria al derecho (Observatorio Distrital de Contratación y Lucha Anticorrupción, 2024)

**Debida diligencia (due dilligence):** proceso que deben llevar a cabo las entidades para identificar, prevenir, mitigar y explicar cómo abordan los impactos negativos reales y potenciales en sus propias actividades, su cadena de suministro y otras relaciones comerciales. (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

**Debida diligencia en el conocimiento de la contraparte:** proceso que le permite a la entidad conocer aspectos relevantes de sus contrapartes, sean partes vinculadas o relacionadas, para poder gestionar el riesgo que cualquier vinculación o relacionamiento genera. (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

**Debida diligencia simplificada.** Aplica cuando el análisis de riesgo determina que la contraparte, la operación o la relación institucional presenta una exposición baja a los riesgos para la integridad pública. Permite reducir la intensidad de las medidas de verificación sin eliminar la identificación básica ni el seguimiento. Si el nivel de riesgo cambia, la entidad debe escalar al nivel correspondiente (GAFI, Nota Interpretativa de la Recomendación 1, numeral 15, 2012; GAFI, Recomendación 10, 2012).

**Debida diligencia estándar.** Nivel de referencia que se aplica cuando el perfil de riesgo no justifica reducir ni intensificar las medidas. Comprende la verificación de identidad, existencia legal y capacidad operativa de la contraparte; la comprensión del propósito de la relación; la

identificación de la estructura de control cuando aplique; y el seguimiento durante la vigencia del vínculo (GAFI, Recomendación 10, 2012; Ley 1121 de 2006, art. 27; Ley 2195 de 2022, art. 12; Secretaría General, Lineamientos Técnicos Distritales, Anexo al Decreto 1122 de 2024, sección 4.1.3).

**Debida diligencia ampliada.** Se activa cuando la contraparte o la operación presenta factores de riesgo elevado, entre ellos la condición de Persona Expuesta Políticamente (PEP), la presencia en listas vinculantes o restrictivas, o señales de alerta no descartadas mediante la diligencia estándar. Exige medidas adicionales de verificación, documentación de decisiones y aprobación de un nivel jerárquico superior antes de establecer o continuar la relación (GAFI, Recomendaciones 10 y 12, 2012; Secretaría General, Lineamientos Técnicos Distritales, sección 4.1.3).

**Declaración de impedimento:** Es la manifestación obligatoria que realiza un servidor público cuando identifica que se encuentra incurso en una causal que puede afectar su imparcialidad, con el fin de apartarse del conocimiento de un asunto. (Artículo 11 de la ley 1437 de 2011)

**Delito fuente:** según el artículo 323 de la Ley 599 de 2000, son delitos fuente del lavado de activos: tráfico de migrantes, trata de personas, extorsión, enriquecimiento ilícito, secuestro extorsivo, rebelión, tráfico de armas, tráfico de menores de edad, financiación del terrorismo y administración de recursos relacionados con actividades terroristas, tráfico de drogas tóxicas, estupefacientes o sustancias sicotrópicas, delitos contra el sistema financiero, delitos contra la administración pública, contrabando, contrabando de hidrocarburos o sus derivados, fraude aduanero o favorecimiento y facilitación del contrabando, favorecimiento de contrabando de hidrocarburos o sus derivados, en cualquiera de sus formas. (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

**Financiación de la Proliferación de Armas de Destrucción Masiva (FP):** fondos u otros activos a disposición, directa o indirectamente, de o para el beneficio de, alguna persona o entidad designada por o bajo la autoridad del Consejo de Seguridad de las Naciones Unidas dentro del Capítulo VII de la Carta de las Naciones Unidas, en lo relativo a la prevención, represión e interrupción de la proliferación de armas de destrucción masiva y su financiamiento. La Financiación de la Proliferación puede darse por: recaudación, transmisión, utilización. (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

**Financiación del Terrorismo (FT):** De acuerdo con el artículo 345 del Código Penal Colombiano modificado por el artículo 16 de la Ley 1453 de 2011, la financiación del terrorismo se define como: "el que directa o indirectamente provea, recolecte, entregue, reciba, administre, aporte, custodie o guarde fondos, bienes o recursos, o realice cualquier otro acto que promueva, organice, apoye, mantenga, financie o sostenga económicamente a grupos de delincuencia organizada, grupos armados al margen de la ley o a sus integrantes, o a grupos terroristas nacionales o extranjeros, o a terroristas nacionales o extranjeros, o a actividades terroristas". La Financiación del Terrorismo puede darse por: recaudación, transmisión, utilización. (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

- **Recaudación:** consiste en la búsqueda de fuentes de financiación por las organizaciones terroristas, bien sean de origen legal, como los aportes de los Estados, individuos, entidades, organizaciones y donantes en general que apoyan su causa o son engañados, así como recursos provenientes de cualquier actividad delictiva, fondos que generalmente

circulan en efectivo. (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

- **Transmisión:** es la fase intermedia que busca poner el dinero recaudado a disposición de la organización terrorista, quedando simplemente la espera de su utilización final; corresponde al movimiento de los fondos a través de distintas técnicas, se trata de ocultar sus movimientos y destino final. (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).
- **Utilización:** fase donde los fondos se utilizan básicamente para la financiación de la logística estructural de la organización o la logística operativa en materia de planeación y ejecución de actos terroristas.(Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

**Fraude:** errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realiza por terceros, externos y la organización es la víctima. (A partir de ISO37001:2025). (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

**Función de cumplimiento:** función que debe distribuirse dentro de la organización que asigna a una persona, grupo o dependencia la responsabilidad de adoptar medidas para promover el cumplimiento interno, administrar los riesgos para la integridad pública de conformidad con las políticas institucionales de gestión de riesgos, apoyar los procesos de evaluación de los Sistemas de Gestión del Riesgo, realizar un control de segunda línea y asesorar a la Alta Dirección en el direccionamiento estratégico de la organización desde un enfoque basado en riesgos para proteger la integridad pública. (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

**Grupo de Acción Financiera Internacional (GAFI):** es un ente intergubernamental establecido en 1989 cuyo objetivo es fijar estándares y promover la implementación efectiva de medidas legales, regulatorias y operativas para combatir el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva, y otras amenazas a la integridad del sistema financiero internacional. (Unidad de Información y Análisis Financiero (UIAF), s.f.)

**Grupo de Acción Financiera de Latinoamérica (GAFILAT)**: es una organización intergubernamental de base regional que agrupa a 18 países de América del Sur, Centroamérica y América del Norte. El GAFILAT fue creado para prevenir y combatir el lavado de activos, financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva, a través del compromiso de mejora continua de las políticas nacionales contra estos flagelos y la profundización en los distintos mecanismos de cooperación entre los países miembros. (Grupo de Acción Financiera de Latinoamérica (GAFILAT), s.f.)

**Lavado de activos:** el artículo 323 de la Ley 599 de 2000, define el delito de lavado de activos como la conducta desplegada por quien *"adquiera, resguarde, invierta, transporte, transforme, almacene, conserve, custodie o administre bienes que tengan su origen mediato o inmediato en actividades, o vinculados con el producto de delitos ejecutados bajo concierto para delinquir, o les dé a los bienes provenientes de dichas actividades apariencia de legalidad o los legalice, oculte o encubra la verdadera naturaleza, origen, ubicación, destino, movimiento o derecho sobre tales bienes o realice cualquier otro acto para ocultar o encubrir su origen ilícito"*. El Lavado de

Activos puede darse por: colocación, ocultamiento e integración (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

- **Colocación:** es la disposición del dinero proveniente de actividades delictivas. Durante esta fase inicial, el determinador o autor introduce sus fondos ilegales en actividades legales o aparentemente legales, bien a través del sistema financiero o de otros tipos de negocios o contratos, tanto nacionales como internacionales. (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).
- **Ocultamiento:** es la separación de fondos ilícitos de su fuente mediante una serie de transacciones, cuyo fin es desdibujar la transacción ilícita original. Esta etapa supone la conversión de los fondos procedentes de actividades ilícitas a otra forma y crear esquemas complejos de transacciones financieras para disimular el rastro documentado, la fuente y la propiedad de los fondos. (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).
- **Integración:** es dar apariencia legítima a riqueza ilícita mediante el reingreso en la economía con transacciones comerciales o personales que aparentan ser normales. Esta fase conlleva la colocación de los fondos lavados de vuelta en la economía para crear una percepción de legitimidad. El lavador podría optar por invertir los fondos en bienes raíces, artículos de lujo o proyectos comerciales, entre otras. (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

**Operación Intentada:** Se configura cuando se tiene conocimiento de la intención de una persona de realizar una operación, pero no se perfecciona por cuanto quien intenta llevarla a cabo desiste de la misma o porque los controles establecidos o definidos por la empresa, no permitieron realizarla. (Unidad de Información y Análisis Financiero (UIAF), s.f., pág. 42)

**Operación Sospechosa**: Es aquella operación que por su número, cantidad o características no se enmarca dentro de las prácticas normales del negocio de una industria o de un sector determinado, además, por los usos y costumbres de la actividad que se trate esta no ha podido ser razonablemente justificada. (Unidad de Información y Análisis Financiero (UIAF), s.f., pág. 42)

**Persona Expuesta Políticamente (PEP):** Persona que, por razón de su cargo, posición o funciones, maneja recursos públicos, tiene poder de disposición sobre estos, ejerce una función pública prominente o desempeña funciones prominentes en una organización internacional, circunstancia que puede generar una mayor exposición al riesgo de LA/FT. Para efectos de su identificación, se tendrán en cuenta las categorías y condiciones establecidas en la normativa aplicable, incluidas las PEP nacionales, extranjeras y de organizaciones internacionales. La condición de PEP se mantiene durante el ejercicio del cargo y por los dos (2) años siguientes a su dejación, renuncia, despido, declaración de insubsistencia del nombramiento o cualquier otra forma de desvinculación, en los términos previstos en la normativa aplicable. Conforme al Decreto 1081 de 2015, modificado por el Decreto 830 de 2021.

**Recusación:** Es el mecanismo mediante el cual un tercero, dentro de una actuación administrativa o judicial, solicita que un servidor público o autoridad se aparte del conocimiento de un asunto, al considerar que existe una causal que compromete su imparcialidad. (Artículo 11 de la ley 1437 de 2011).

**Riesgos para la integridad pública:** Toda actuación o decisión de las y los servidores públicos, así como de otros colaboradores de las entidades públicas que privilegien el interés particular sobre el general, asociadas a conductas no deseadas que van en contravía de los valores del servicio público. Incluido, también, el riesgo de que la integridad de la entidad sea utilizada para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas. (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

**Reporte de ausencia de operaciones o de transacciones**: existe si durante el período de reporte no fueron identificadas operaciones sospechosas, operaciones intentadas u operaciones rechazadas que contengan características que les otorgue el carácter de sospechosas y que deban ser de conocimiento inmediato de la UIAF. En tal caso, la entidad reportante debe realizar el reporte de ausencia de ROS (reporte negativo) a través de SIREL, siempre y cuando su obligatoriedad esté dentro de las especificaciones técnicas del anexo o normatividad aplicable al sector, en las fechas establecidas para el envío del reporte. (Unidad de Información y Análisis Financiero - UIAF, 2020, pág. 5)

**Reporte de Operación Sospechosa:** Es un informe que los sujetos obligados deben enviar a la UIAF cada vez que detectan o identifiquen una operación sospechosa. Un ROS no es una denuncia. El ROS es anónimo, reservado, constituye un criterio orientador y no una prueba judicial, no es un testimonio y no genera ningún tipo de responsabilidad. Adicionalmente, un ROS no representa una sentencia penal. (Unidad de Información y Análisis Financiero (UIAF), s.f., pág. 43)

**Segmentación:** Es el proceso por medio del cual se lleva a cabo la separación de elementos en grupos homogéneos al interior de ellos y heterogéneos entre ellos. La separación se fundamenta en el reconocimiento de diferencias significativas en sus características (Superintendencia Financiera de Colombia, 2020).

**Señal de alerta:** Son aquellas situaciones que al ser analizadas se salen de los comportamientos particulares de los clientes o del mercado, considerándose atípicas y que, por tanto, requieren mayor análisis para determinar si existe una posible operación de lavado de activos o financiación del terrorismo. Lo que hace una señal de alerta es el reconocimiento de una posible operación de lavado de activos o financiación del terrorismo. A este respecto, es importante mencionar que no todas las operaciones que presentan comportamientos atípicos e inusuales son efectuadas por organizaciones criminales, por lo cual, la identificación señales de alerta no es motivo suficiente para generar un reporte inmediato a la UIAF. (Unidad de Información y Análisis Financiero (UIAF), 2014)

**Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP:** esquema que define la interrelación e interacción de diferentes elementos para asegurar una gestión integral de los riesgos que afectan la integridad pública. El SIGRIP se articula con la Política para la Gestión Integral de Riesgos (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

**Sistema de Reporte en Línea _SIREL**:es una herramienta web que permite a las entidades reportantes cargar los reportes de acuerdo con las obligaciones establecidas en la normatividad de cada sector, de forma eficiente y segura, disponible las 24 horas al día, siete días a la semana y 365 días al año. (Unidad de Información y Análisis Financiero., 2022)

**Soborno:** ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar. (A partir de ISO37001:2025). (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

**Soborno entrante:** ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida a un servidor de la entidad. (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

**Soborno saliente:** ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida por parte de servidores públicos a otros en nombre de la entidad. (Anexo 2 Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7).

# Siglas y Abreviaturas

| Sigla o abreviatura | Denominación completa |
|---|---|
| **ALA/CFT/CFP** | Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva. |
| **CONPES** | Consejo Nacional de Política Económica y Social. |
| **COSO** | Comité de Organizaciones Patrocinadoras de la Comisión Treadway, por su denominación en inglés *Committee of Sponsoring Organizations of the Treadway Commission*. |
| **COSO ERM** | Marco de Gestión de Riesgos Empresariales del COSO, por su denominación en inglés *Enterprise Risk Management*. |
| **DAFP** | Departamento Administrativo de la Función Pública. |
| **DASCD** | Departamento Administrativo del Servicio Civil Distrital. |
| **DEA** | Administración de Control de Drogas de los Estados Unidos, por su denominación en inglés *Drug Enforcement Administration*. |
| **FP** | Financiación de la Proliferación de Armas de Destrucción Masiva. |
| **FPADM** | Financiación de la Proliferación de Armas de Destrucción Masiva. Esta sigla se conservará cuando forme parte de la denominación oficial de una fuente, instrumento o régimen que la utilice. |
| **FT** | Financiación del Terrorismo. |
| **GAFI** | Grupo de Acción Financiera Internacional. |
| **GAFILAT** | Grupo de Acción Financiera de Latinoamérica. |
| **IA** | Inteligencia Artificial. |

| Sigla o abreviatura | Denominación completa |
|---|---|
| **ISO** | Organización Internacional de Normalización, por su denominación en inglés *International Organization for Standardization*. |
| **KPI** | Indicador Clave de Desempeño, por su denominación en inglés *Key Performance Indicator*. |
| **KRI** | Indicador Clave de Riesgo, por su denominación en inglés *Key Risk Indicator*. |
| **LA** | Lavado de Activos. |
| **LA/FT** | Lavado de Activos y Financiación del Terrorismo. |
| **LA/FT/FP** | Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva. |
| **MECI** | Modelo Estándar de Control Interno. |
| **MGJA** | Modelo de Gestión Jurídica Anticorrupción |
| **MIPG** | Modelo Integrado de Planeación y Gestión. |
| **OCDE** | Organización para la Cooperación y el Desarrollo Económicos. |
| **ODCLA** | Observatorio Distrital de Contratación y Lucha Anticorrupción. |
| **OFAC** | Oficina de Control de Activos Extranjeros del Departamento del Tesoro de los Estados Unidos, por su denominación en inglés *Office of Foreign Assets Control*. |
| **ONU** | Organización de las Naciones Unidas. |
| **OTI** | Oficina de Tecnologías de la Información. Esta sigla deberá utilizarse únicamente cuando corresponda a la denominación oficial de la dependencia de la entidad respectiva. |
| **PEP** | Persona Expuesta Políticamente. |
| **PQRSD** | Peticiones, Quejas, Reclamos, Sugerencias y Denuncias. |
| **PTEP** | Programa de Transparencia y Ética Pública. |
| **PTEE** | Programa de Transparencia y Ética Empresarial. |
| **REDAM** | Registro de Deudores Alimentarios Morosos. |
| **RNMC** | Registro Nacional de Medidas Correctivas. |
| **ROI** | Reporte Interno de Operación Inusual. |

| Sigla o abreviatura | Denominación completa |
|---|---|
| **ROS** | Reporte de Operación Sospechosa. |
| **RUB** | Registro Único de Beneficiarios Finales. |
| **RUES** | Registro Único Empresarial y Social. |
| **RUP** | Registro Único de Proponentes. |
| **RUT** | Registro Único Tributario. |
| **SARLAFT** | Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo. |
| **SECOP** | Sistema Electrónico para la Contratación Pública. |
| **SIDEAP** | Sistema de Información Distrital del Empleo y la Administración Pública. |
| **SIGRIP** | Sistema de Gestión de Riesgos para la Integridad Pública. |
| **SIPLAFT** | Sistema Integral para la Prevención y Control del Lavado de Activos y la Financiación del Terrorismo. Se utilizará únicamente cuando corresponda al régimen sectorial aplicable. |
| **SIRI** | Sistema de Información de Registro de Sanciones y Causas de Inhabilidad de la Procuraduría General de la Nación. |
| **SIREL** | Sistema de Reporte en Línea administrado por la Unidad de Información y Análisis Financiero. |
| **UE** | Unión Europea. |
| **UIAF** | Unidad de Información y Análisis Financiero. |
| **UNCAC** | Convención de las Naciones Unidas contra la Corrupción, por su denominación en inglés *United Nations Convention against Corruption*. |
| **UNODC** | Oficina de las Naciones Unidas contra la Droga y el Delito, por su denominación en inglés *United Nations Office on Drugs and Crime*. |

# ¿Qué es el SIGRIP?

El Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) es el conjunto estructurado de políticas, procedimientos, controles y mecanismos de seguimiento que las entidades públicas implementan para identificar, valorar, tratar y monitorear los riesgos que amenazan su integridad institucional, abordando de manera integrada cinco amenazas: soborno, fraude, conflicto de interés, corrupción, y lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva (LA/FT/FP) (Departamento Administrativo de la Función Pública, 2025)

Su existencia responde al mandato del artículo 31 de la Ley 2195 de 2022, que modificó el artículo 73 de la Ley 1474 de 2011, al establecer la obligación de las entidades públicas de implementar Programas de Transparencia y Ética Pública (PTEP) con enfoque basado en riesgos, reglamentada mediante el Decreto 1122 de 2024. En este marco, el SIGRIP desarrolla el componente programático de administración del riesgo del PTEP, con el propósito de vincular en un esquema articulado herramientas e instrumentos ya existentes "para una gestión integral de prevención, detección y respuesta frente a riesgos de corrupción, fraude o soborno; de los conflictos de interés, los incumplimientos al código de integridad, riesgos fiscales, de lavado de activos y otros que puedan afectar la imagen y confianza institucional de cara a la ciudadanía" (Departamento Administrativo de la Función Pública, 2025). Para el Distrito Capital, su implementación se desarrolla en el marco de los Lineamientos Técnicos Distritales para la implementación de los PTEP.

# ¿Cómo se articula el SIGRIP con el PTEP?

El Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) constituye una herramienta para la implementación del componente programático del Programa de Transparencia y Ética Pública (PTEP).

Mientras el PTEP define la estrategia institucional para la lucha contra la corrupción y establece los elementos mínimos que deben desarrollar las entidades públicas, el SIGRIP proporciona orientaciones técnicas y metodológicas para la implementación de aquellos componentes relacionados con la gestión de riesgos para la integridad pública.

En este sentido, el SIGRIP desarrolla y articula mecanismos asociados a la gestión de riesgos de corrupción, fraude, soborno, conflictos de interés, debida diligencia, canales de denuncia, función de cumplimiento y riesgos de LA/FT/FP, contribuyendo al cumplimiento de las acciones estratégicas previstas en el componente programático del PTEP.

Por tanto, el SIGRIP no reemplaza al Programa de Transparencia y Ética Pública ni constituye un instrumento independiente de este, sino que actúa como una herramienta complementaria que facilita su implementación y fortalecimiento.

# ¿Cómo se articula el SIGRIP con MIPG y MECI?

El SIGRIP se articula con el Modelo Integrado de Planeación y Gestión (MIPG) y con el Modelo Estándar de Control Interno (MECI), aprovechando las capacidades institucionales existentes para fortalecer la prevención y gestión de riesgos asociados a la integridad pública.

En el marco del MIPG, el SIGRIP incorpora elementos relacionados con las políticas de Integridad, Planeación Institucional, Gestión del Conocimiento, Participación Ciudadana, Transparencia y Acceso a la Información Pública, Gestión Documental, Control Interno y Gestión Estratégica del Talento Humano, promoviendo una visión transversal de la integridad en la gestión pública.

Por su parte, el MECI aporta la estructura de control necesaria para garantizar que los riesgos identificados sean adecuadamente gestionados mediante controles efectivos, mecanismos de monitoreo, seguimiento y evaluación continua.

De igual forma, el SIGRIP adopta el esquema de líneas de aseguramiento promovido por MIPG y MECI, asignando responsabilidades diferenciadas para la ejecución, supervisión y evaluación de sus componentes, con el propósito de fortalecer la gobernanza institucional, la gestión basada en riesgos y la mejora continua de los mecanismos de prevención de la corrupción (Departamento Administrativo de la Función Pública, 2025)

# Capítulo 1 Gestión del Riesgo para las Amenazas de Fraude, Soborno, Corrupción e Inadecuada Gestión del Conflicto de Interés

## 1.1 Gestión del riesgo de las amenazas de Fraude Interno, Soborno y Corrupción.

### 1.1.1. Contexto del componente.

Desde 2014, con la expedición de la Guía de Gestión de Riesgos versión 4 del DAFP, las entidades distritales cuentan con lineamientos para la gestión de los riesgos de corrupción. No obstante, en el marco de la articulación de acciones y esfuerzos, estos riesgos se integran con manifestaciones específicas como el fraude interno, el soborno y la inadecuada gestión de conflictos de interés, lavado de activos la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva consolidándose bajo la denominación de Riesgos de Integridad Pública.

En este capítulo estableceremos las pautas para gestionar las amenazas de fraude interno, corrupción y soborno y como estas se encuentran asociados al factor de riesgo Talento Humano, en la medida en que se relacionan al comportamiento y la conducta del servidor o contratista. Por su parte, el Fraude Externo constituye un riesgo netamente operativo, al que la Entidad se expone por conductas desplegadas por terceros; por esta razón, este tipo de fraude se considera, ante todo, un riesgo general de gestión.

La gestión de los riesgos frente a estas amenazas permite a la entidad detectar y mitigar situaciones que pueden impedir el logro de los objetivos y metas institucionales y garantizar el buen uso de los recursos públicos, así como establecer acciones de mayor impacto para evitar hechos de corrupción.

Para efectos de la presente Estrategia, es importante diferenciar las amenazas de los riesgos para la integridad pública. Las amenazas corresponden a los fenómenos o situaciones que pueden afectar la integridad pública, mientras que los riesgos corresponden a los eventos que cada entidad identifica y formula, de acuerdo con su contexto, procesos y nivel de exposición, frente a dichas amenazas. En consecuencia, una misma amenaza puede dar lugar a diferentes riesgos según las características y operaciones de cada entidad.

La metodología para la gestión de los riesgos se mantiene y aplica de la misma forma para los riesgos de integridad pública. En consecuencia, comprende las etapas de identificación, valoración, tratamiento, monitoreo y comunicación de los riesgos.

Para gestionar estas amenazas es importante poder identificar a través de la misionalidad, los objetivos estratégicos, la cadena de valor y los procesos de cada entidad de qué forma se puede materializar un riesgo de integridad pública. En el anexo modelo de madurez se establecen las pautas para gestionar dichos riesgos (Anexo 2. Modelo de Madurez).

Ahora bien, la materialización del riesgo no debe confundirse con la ocurrencia de un delito, falta disciplinaria o conducta que genere responsabilidad fiscal. Es posible que un riesgo se materialice esto es, que produzca impactos y consecuencias negativas para la organización incluso antes de que se inicie o formalice un proceso sancionatorio. Los riesgos materializados requieren acciones inmediatas por lo cual es importante consignar en la matriz de riesgos el plan de contingencia y los responsables de su ejecución.

Con el propósito de apoyar la identificación de riesgos, se incorpora como anexo (Anexo 3. Ejemplos de riesgos y controles frente a las amenazas de soborno, fraude interno, corrupción y conflicto de interés) una relación de riesgos y controles a manera de referencia, teniendo en cuenta que pueden existir otros controles adicionales para mitigar los riesgos, así como riesgos distintos que respondan a la naturaleza y misionalidad de cada entidad.

Para fortalecer la gestión institucional y anticipar eventos que puedan afectar el cumplimiento de los objetivos, se presenta el siguiente conjunto de indicadores orientados a la identificación, el monitoreo y el control de riesgos de integridad y de gestión. Estos indicadores permiten evaluar de manera periódica la exposición al riesgo en los procesos críticos, facilitando la detección de alertas tempranas, la toma de decisiones informadas y la implementación de acciones preventivas y correctivas. Así mismo, constituyen un insumo clave para el seguimiento del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), promoviendo la transparencia, la eficiencia operativa y la mejora continua en la Entidad.

Cabe precisar que los ejemplos de indicadores aquí presentados no deben asociarse de manera automática con la existencia de irregularidades. Sus resultados deben analizarse a la luz del contexto particular, la modalidad contractual y las características propias de cada entidad, de modo que su interpretación sea razonable, objetiva y ajustada a la realidad institucional.

**Ejemplos de Indicadores de riesgos de Integridad:**

- Número de contratos suscritos mediante modalidades de contratación sin proceso competitivo de selección respecto al total de contratos celebrados en el período. Este indicador puede constituir una señal para analizar la distribución de las modalidades de contratación utilizadas por la entidad, la justificación de su aplicación y la suficiencia de los mecanismos de control establecidos.
- Porcentaje del valor total contratado con un mismo proveedor, unión temporal o consorcio durante el último año. Su comportamiento puede aportar elementos para evaluar los niveles de concentración de la contratación y analizar las condiciones del mercado, la oferta disponible y las dinámicas de participación de proveedores.
- Número de modificaciones, adiciones o prórrogas realizadas a los contratos respecto al total de contratos suscritos. Este indicador puede constituir una señal para examinar

aspectos relacionados con la planeación contractual, la definición de necesidades, la gestión de riesgos y las condiciones de ejecución de los contratos.

- Porcentaje de procesos de selección competitiva en los que únicamente un proponente resulta habilitado o adjudicatario respecto al total de procesos realizados en el período. Los resultados de este indicador pueden requerir el análisis de factores asociados a las condiciones del proceso, la participación del mercado, los requisitos establecidos y los niveles de concurrencia de oferentes.
- Número de procesos de contratación con hallazgos identificados por auditoría interna u organismos de control respecto al total de procesos evaluados en el período. Este indicador permite identificar procesos que pueden requerir revisión y fortalecimiento de controles relacionados con la planeación, ejecución, supervisión o seguimiento contractual.
- Número de quejas relacionadas con presuntos incumplimientos en la publicación de documentos contractuales en las plataformas oficiales. Su comportamiento puede constituir una señal para revisar la oportunidad, integridad y cumplimiento de los procedimientos de publicación y divulgación de la información contractual.
- Número de quejas o denuncias por presuntos actos de corrupción recibidas durante el período de medición. Este indicador proporciona información para el análisis de riesgos institucionales y del funcionamiento de los mecanismos de recepción, gestión y seguimiento de quejas o denuncias.
- Índice de rotación de personal en áreas críticas de la entidad (por ejemplo, contratación, tesorería o gestión financiera). Puede constituir una señal para analizar factores relacionados con la continuidad operativa, la transferencia de conocimiento, la gestión del talento humano y la estabilidad de los procesos.
- Número de quejas recibidas relacionadas con presuntos cobros irregulares para la realización de trámites, servicios o expedición de autorizaciones. Este indicador puede aportar elementos para identificar situaciones que requieran verificación, fortalecimiento de controles o revisión de los procedimientos asociados a la prestación de los servicios.
- Porcentaje de servidores públicos obligados que han presentado las declaraciones de bienes y rentas y conflictos de interés respecto al total de obligados. Este indicador permite monitorear el cumplimiento de las obligaciones establecidas y constituye un insumo para los procesos de seguimiento y control a cargo de las dependencias competentes.

**Ejemplos de indicadores de riesgos de Gestión**:

- Porcentaje de ejecución presupuestal realizada en los últimos periodos de la vigencia fiscal o cerca de los plazos normativos establecidos. Este indicador puede constituir una señal de alerta sobre posibles concentraciones de la ejecución en determinados periodos, por lo que requiere analizar las condiciones de planeación, contratación y gestión presupuestal de la entidad.
- Número de hallazgos recurrentes en informes de auditoría interna o de organismos de control. La recurrencia de hallazgos puede evidenciar aspectos susceptibles de mejora en los procesos institucionales, controles existentes o en la implementación y seguimiento de acciones correctivas, preventivas o de mejora.

- Porcentaje de pagos realizados después de la fecha de vencimiento establecida. Un resultado elevado puede indicar la necesidad de analizar factores asociados a la gestión financiera, los procedimientos de revisión y aprobación, la disponibilidad de soportes o las dinámicas operativas del proceso de pago.
- Tiempo promedio de respuesta a peticiones, quejas, reclamos, sugerencias y denuncias (PQRSD) superior a los términos establecidos. Este indicador puede alertar sobre posibles dificultades en la gestión de las solicitudes ciudadanas, por lo que resulta necesario evaluar las causas asociadas a la capacidad operativa, la gestión documental o los flujos internos de atención.
- Porcentaje de indisponibilidad o interrupción de servicios digitales y plataformas tecnológicas. Su comportamiento permite identificar la necesidad de analizar la capacidad de respuesta ante incidentes tecnológicos, la continuidad de la operación y la efectividad de los mecanismos de soporte y recuperación.
- Número de fallas identificadas en los procesos de conciliación bancaria diaria. Un incremento en este indicador puede señalar la conveniencia de revisar la confiabilidad de los registros, los procedimientos de conciliación, la interoperabilidad entre sistemas y los controles asociados al proceso financiero.
- Porcentaje de servidores públicos con evaluación de desempeño actualizada respecto al total de la planta de personal. Este indicador permite analizar el avance en la gestión del desempeño y constituye un insumo para evaluar la oportunidad de los procesos de seguimiento, retroalimentación y desarrollo del talento humano.
- Porcentaje de bienes inventariados y verificados respecto al total de bienes registrados. Este indicador aporta elementos para analizar la efectividad de los controles sobre los activos institucionales y la oportunidad de los procesos relacionados con la administración, actualización y verificación de inventarios.

### 1.1.2 Políticas Antisoborno y Antifraude.

Las entidades del distrito de acuerdo con lo dispuesto en la Guía Gestión Integral de Riesgo V.7, deben incluir en la Política para la Gestión Integral de Riesgos el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) y sus distintos componentes, así como cada uno de los elementos adicionales con que debe contar cada entidad, y que en su conjunto derivan en un sistema integral de gestión del riesgo.

El SIGRIP incluye como herramientas las políticas **Antisoborno y Antifraude** como medida de control por lo cual es importante formular, adoptar e implementar dichas políticas que contribuyan a la integridad.

El enfoque de estas políticas deberá asegurar el compromiso expreso de la Alta Dirección y de todas las dependencias para que trabajen de manera conjunta y especializada, garantizando así la efectividad en la prevención, mitigación y control de los riesgos, manteniendo la integridad y la transparencia en todas las operaciones de la entidad.

La Políticas de Administración de Riesgos **Antisoborno y Antifraude** de la entidad debe fijar pautas dirigidas a todas las dependencias, en sus procesos, procedimientos, a sus funcionarios

y contratistas, así como a terceros con los que se establecen o mantienen relaciones contractuales, en lo de su competencia y en lo que no sea contrario a la Ley.

A continuación, se presenta un ejemplo de carácter orientador sobre los mínimos (declaración, pautas comportamentales y consecuencias) que puede contener una política:

## Declaración de compromisos Política de Riesgos Antisoborno

*La Alta Dirección y todos los servidores públicos, contratistas, colaboradores y grupos de valor de la (Nombre de la Entidad) en cumplimiento de los principios de legalidad, transparencia, integridad, responsabilidad y ética pública, declara su compromiso firme e irrevocable con la prevención, detección, gestión y rechazo de cualquier forma de soborno, directo o indirecto, en el desarrollo de sus funciones, procesos y relaciones con sus grupos de valor.*

*En este sentido, la Entidad adopta una política de cero tolerancia frente al soborno, entendiendo este como cualquier ofrecimiento, promesa, entrega, solicitud o aceptación indebida de dinero, bienes, favores, beneficios o ventajas, con el fin de influir de manera inapropiada en decisiones o actuaciones institucionales.*

## Declaración de compromiso Política de Riesgos Antifraude

*La (Nombre de la Entidad), en cumplimiento del principio de defensa del patrimonio público, declara su compromiso institucional con la prevención, detección, control y mitigación de los riesgos de fraude, entendiendo el fraude como errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio propio o de terceros, ya sea de origen interno, cuando involucra a colaboradores de la Entidad, o externo, cuando es cometido por terceros ajenos a la organización, siendo esta la víctima.*

*En consecuencia, la Alta Dirección y todos los servidores públicos, contratistas, colaboradores y partes interesadas manifiestan su compromiso con una política de cero tolerancia frente al fraude, en cualquiera de sus modalidades.*

*En cumplimiento de la **Política de Riesgos Antisoborno, Antifraude**, los servidores se comprometen a actuar con integridad, transparencia, responsabilidad y legalidad en el ejercicio de sus funciones, observando las siguientes **pautas de comportamiento**:*

Los servidores deberán:

1. Conocer, comprender y cumplir las disposiciones, procedimientos, controles y lineamientos establecidos en las Políticas de Riesgos Antisoborno y Antifraude, así como en la normativa vigente aplicable.
2. Desempeñar sus funciones con rectitud, imparcialidad, honestidad, diligencia y buena fe en todas las actuaciones, decisiones, procesos y operaciones que realicen en el marco de sus competencias.
3. Prevenir, identificar, evaluar y gestionar los riesgos de soborno y fraude en las actividades, decisiones y procesos que estén bajo su responsabilidad.
4. Reportar de manera inmediata, veraz y oportuna al superior jerárquico, al oficial de cumplimiento, a los canales de denuncia establecidos o a la instancia competente, cualquier ofrecimiento, solicitud, promesa, entrega, indicio o situación que pueda

constituir soborno, fraude o conducta contraria a los principios de transparencia y legalidad.
5. Abstenerse de participar en decisiones o actuaciones cuando exista un conflicto de interés, informándolo oportunamente conforme a los procedimientos internos.
6. Suministrar información completa, exacta y verificable cuando sea requerida en procesos de supervisión, auditoría, investigación o evaluación de riesgos de soborno y fraude.
7. Mantener la confidencialidad de la información relacionada con denuncias, reportes, investigaciones o análisis sobre posibles actos de soborno o fraude.
8. Custodiar y utilizar de manera adecuada los recursos, bienes, activos, información y sistemas de la entidad, evitando su uso indebido o no autorizado.
9. Garantizar la veracidad, integridad y oportunidad de los registros contables, financieros, administrativos y operativos, de conformidad con las políticas y normas aplicables.
10. Participar activamente en los programas de capacitación, sensibilización y actualización en materia de ética, integridad y prevención del soborno y el fraude promovidos por la entidad.

Los servidores se abstendrán de:

1. Solicitar, aceptar, ofrecer, prometer, entregar, ejecutar, facilitar, permitir o encubrir, directa o indirectamente, actos de soborno, fraude, falsificación, apropiación indebida o cualquier otra conducta irregular, sin importar su forma o cuantía.
2. Utilizar o valerse de su cargo, función, posición o acceso a información privilegiada para obtener ventajas personales o para terceros, en contravención de los principios de integridad y legalidad.
3. Manipular, alterar, ocultar o destruir documentos, registros, sistemas de información o evidencias, con el propósito de encubrir hechos, engañar, obtener beneficios indebidos o evadir controles internos.
4. Realizar pagos de facilitación, contribuciones indebidas o cualquier otro desembolso no autorizado que tenga como finalidad acelerar, influir o asegurar trámites o decisiones.
5. Omitir, retrasar o impedir el reporte de hechos, indicios o actos de soborno o fraude de los que tenga conocimiento en el ejercicio de sus funciones.
6. Utilizar los recursos, bienes, activos o información de la entidad para fines personales o no autorizados.
7. Tomar represalias, intimidar o ejercer presiones contra personas que, de buena fe, denuncien, reporten o colaboren en la detección e investigación de posibles actos de soborno o fraude.
8. Participar en decisiones o actuaciones que generen conflictos de interés sin haberlos declarado oportunamente conforme a los procedimientos internos.

**Consecuencias del incumplimiento.**

El incumplimiento de los lineamientos, procedimientos o controles asociados a la gestión de riesgos será puesto en conocimiento de las instancias o autoridades competentes cuando los hechos puedan tener relevancia administrativa, disciplinaria, contractual, fiscal, penal o de cualquier otra naturaleza prevista en la normatividad vigente.

La determinación de responsabilidades corresponderá exclusivamente a las autoridades competentes, con observancia del debido proceso, el derecho de defensa y las demás garantías constitucionales y legales aplicables.

## 1.2. Conflicto de interés

En el marco del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), el conflicto de interés se reconoce como una de las principales amenazas que pueden afectar la imparcialidad, la transparencia y la toma de decisiones en las entidades públicas. Su gestión se inscribe dentro del enfoque basado en riesgos para la integridad, el cual busca anticipar y prevenir situaciones que puedan derivar en la afectación del interés general, particularmente cuando se presentan condiciones que facilitan la materialización de conductas indebidas. En este sentido, la inadecuada gestión del conflicto de interés ha sido identificada como una causa directa de riesgos de integridad, en la medida en que puede incidir en decisiones que favorezcan intereses particulares sobre los principios que rigen la función pública.

De acuerdo con la normativa colombiana, el conflicto de interés se presenta cuando el interés general, propio del ejercicio de la función pública, entra en tensión con un interés particular y directo del servidor público, ya sea propio o de su entorno cercano, incluyendo cónyuge, compañero permanente, familiares o socios[2]. Esta situación no constituye en sí misma una irregularidad ni un acto de corrupción; sin embargo, configura un escenario de riesgo que debe ser gestionado oportunamente. Por tanto, el énfasis institucional no debe centrarse únicamente en sancionar su materialización, sino en establecer mecanismos que permitan su identificación temprana y su tratamiento adecuado.

En el ámbito distrital, este proceso se encuentra respaldado por un conjunto de disposiciones constitucionales, legales, reglamentarias y de orientación técnica que han contribuido al fortalecimiento de las capacidades institucionales para prevenir, identificar y gestionar los conflictos de interés. Entre ellas se destacan el artículo 209 de la Constitución Política; la Ley 2013 de 2019; el Decreto Único Sectorial 640 de 2025; el Acuerdo Distrital 782 de 2020; la Directiva Conjunta 004 de 2025 y la Circular DASCD 015 de 2026, en el marco de sus respectivos ámbitos de aplicación.

En este contexto, el riesgo para la integridad no radica en la existencia del conflicto de interés, sino en su falta de declaración, gestión oportuna o tratamiento inadecuado. La gestión del conflicto de interés se materializa a través de mecanismos como la declaración de impedimento y la recusación, los cuales permiten apartar al servidor público del conocimiento de un asunto cuando existen circunstancias que comprometen su imparcialidad.[3] A estos mecanismos se suman herramientas institucionales que facilitan la prevención y control del riesgo, entre las cuales se destaca el Sistema de Información Distrital del Empleo y la Administración Pública (SIDEAP),[4] como plataforma para la declaración y registro de conflictos de interés, bienes y

[2] Ley 1952 de 2019, Código General Disciplinario, art. 44 (conflicto de intereses); disposiciones sobre conflicto de interés; y Ley 1474 de 2011, Estatuto Anticorrupción, en lo relacionado con medidas para la prevención de actos de corrupción asociados a conflictos de interés.
[3] Ley 1437 de 2011, Código de Procedimiento Administrativo y de lo Contencioso Administrativo, arts. 11 y 12 (impedimentos y recusaciones).
[4] Lineamientos para la declaración de bienes, rentas y conflictos de interés y uso del Sistema de Información Distrital del Empleo y la Administración Pública (SIDEAP), Bogotá D.C.

rentas, que permite fortalecer la trazabilidad, el seguimiento y la toma de decisiones informadas en el ámbito distrital[1].

Desde esta perspectiva, la gestión del conflicto de interés debe ser entendida como una función institucional asumida de manera estructurada por las entidades, mediante la definición de políticas, procedimientos y controles que aseguren su adecuada administración. En este marco, el presente apartado tiene como propósito orientar a las entidades en la gestión del conflicto de interés desde un enfoque práctico y basado en riesgos, proporcionando lineamientos para la elaboración de procedimientos, la identificación de niveles de madurez institucional y la implementación de acciones que permitan prevenir, gestionar y controlar este tipo de situaciones en el desarrollo de sus funciones.

### 1.2.1 Recomendaciones para la elaboración de un procedimiento para la adecuada gestión de conflictos de interés

La formulación del procedimiento para la gestión de conflictos de interés debe entenderse como la construcción de un instrumento práctico que permita a la entidad identificar, declarar, gestionar y hacer seguimiento a situaciones que puedan afectar la imparcialidad en la toma de decisiones. Más que un documento formal, se trata de una herramienta de uso cotidiano que debe ser clara, aplicable y articulada con los procesos institucionales.

A continuación, se presentan recomendaciones orientadas a facilitar su diseño e implementación, especialmente en entidades que desarrollan este procedimiento por primera vez:

**Traducir la normativa en situaciones concretas**

El punto de partida consiste en asegurar que todos los actores comprendan qué es un conflicto de interés y cómo se manifiesta en la operación diaria. Para ello, el procedimiento debe traducir la normativa en ejemplos claros y aplicables, evitando definiciones abstractas.

En este ejercicio es clave incorporar las causales de impedimento definidas en la normativa, especialmente aquellas relacionadas con vínculos personales, económicos o relacionales que pueden afectar la imparcialidad.

*Tabla 1 Causales de impedimento*

| ÍTEM | TIPOLOGÍA | DESCRIPCIÓN DE LA SITUACIÓN |
|---|---|---|
| 1 | **Interés directo/Conocimiento previo/Concepto o consejo fuera de la actuación.** | Que el(la) servidor(a) público(a) o colaborador(a) del Estado, tenga interés particular y directo en la regulación, gestión, control o decisión del asunto. Que el(la) servidor(a) público(a) o colaborador(a) del Estado, haya conocido del asunto en oportunidad anterior. Que el(la) servidor(a) público(a) o colaborador(a) del Estado, haya dado consejo o concepto por fuera de la actuación administrativa sobre las cuestiones materia de la misma, o haya intervenido en esta como apoderado(a), agente del Ministerio Público, perito(a) o testigo(a). Que el servidor(a) público(a) o colaborador(a) haya proferido la decisión que está sujeta a su revisión. |

| ÍTEM | TIPOLOGÍA | DESCRIPCIÓN DE LA SITUACIÓN |
|---|---|---|
| 2 | **Relación con las partes.** | Que el(la) servidor(a) público(a) o colaborador(a) del Estado, tenga relación con las partes interesadas en el asunto. |
| 3 | **Heredero o legatario.** | Que él(la) servidor(a) público(a) o colaborador(a) del Estado, sea heredero(a) o legatario(a) de alguna de las personas interesadas en la actuación administrativa. Que el cónyuge, compañero(a) permanente o alguno de sus parientes dentro de los grados de consanguinidad o afinidad establecidos por la normatividad, sea heredero(a) o legatario(a) de alguna de las personas interesadas en la actuación administrativa. |
| 4 | **Amistad o enemistad.** | Que exista enemistad grave por hechos ajenos a la actuación administrativa, o amistad entrañable entre el servidor(a) público(a) o colaborador(a) del Estado y alguna de las personas interesadas en la actuación administrativa, su representante o apoderado(a). |
| 5 | **Curador o tutor del interesado.** | Que el servidor(a) público(a) o colaborador(a) del Estado, sea curador(a) o tutor(a) de la persona interesada en el asunto. Que el cónyuge, compañero(a) permanente o alguno de sus parientes dentro de los grados de consanguinidad o afinidad establecidos por la normatividad, sea curador(a) o tutor(a) de persona interesada en el asunto. |
| 6 | **Organización, sociedad o asociación a la cual perteneció o continúa siendo miembro.** | Que el servidor(a) público(a) o colaborador(a) del Estado, sea socio(a) de alguna de las personas interesadas en la actuación administrativa o su representante o apoderado(a) en sociedad de personas. Ser cónyuge, compañero(a) permanente, o pariente dentro de los grados de consanguinidad o afinidad establecidos por la normatividad, o socio(a) de alguna de las personas interesadas en la actuación administrativa o su representante o apoderado(a) en sociedad de personas. |
| 7 | **Litigio o controversia/decisión administrativa pendiente.** | Que exista litigio o controversia ante autoridades administrativas o jurisdiccionales entre el servidor(a) público(a) o colaborador(a) del Estado y cualquiera de los interesados en la actuación, su representante o apoderado(a). Que exista litigio o controversia ante autoridades administrativas o jurisdiccionales entre el cónyuge, compañero(a) permanente, o alguno de los parientes del servidor(a) público(a) o colaborador(a) y cualquiera de los interesados en la actuación, su representante o apoderado(a). Que el servidor(a) público(a) o colaborador(a) del Estado tenga decisión administrativa pendiente en que se controvierta la misma cuestión jurídica que debe resolver. Tener el cónyuge, compañero(a) permanente o alguno de los parientes dentro de los grados de consanguinidad o afinidad establecidos por la normatividad, decisión administrativa o pleito pendiente en que se controvierta la misma cuestión jurídica que el servidor(a) público(a) o colaborador(a) del Estado debe resolver. |
| 8 | **Denuncia penal, o disciplinaria, o contractual o de negocios.** | Que alguno de los interesados en la actuación, su representante o apoderado(a), haya formulado denuncia penal o disciplinaria contra el servidor(a) público(a) o colaborador(a) del Estado antes de iniciarse la actuación administrativa; o después, siempre que la denuncia se refiera a hechos ajenos a la actuación y que el(la) denunciado(a) se halle vinculado(a) a la investigación penal o disciplinaria. Que el servidor(a) público(a) o colaborador(a) del Estado haya formulado denuncia penal contra una de las personas interesadas en la actuación administrativa o su representante o apoderado(a), o estar aquellos legitimados para intervenir como parte civil en el respectivo proceso penal. Que alguno de los interesados en la actuación, su representante o apoderado(a) haya formulado denuncia penal o disciplinaria contra el cónyuge, compañero(a) permanente del |

| ÍTEM | TIPOLOGÍA | DESCRIPCIÓN DE LA SITUACIÓN |
|---|---|---|
| | | servidor(a) público(a) o colaborador(a) del Estado o alguno de los parientes dentro de los grados de consanguinidad o afinidad establecidos por la normatividad antes de iniciarse la actuación administrativa; o durante su trámite, siempre que la denuncia se refiera a hechos ajenos a la actuación y que el denunciado(a) se halle vinculado(a) a la investigación penal o disciplinaria. Que el cónyuge, compañero(a) permanente o alguno de los parientes dentro de los grados de consanguinidad o afinidad establecidos por la normatividad haya formulado denuncia penal contra una de las personas interesadas en la actuación administrativa o su representante o apoderado(a), o estar aquellos legitimados para intervenir como parte civil en el respectivo proceso penal. |
| **9** | **Acreedor/deudor.** | Que el servidor(a) público(a) o colaborador(a) del Estado, sea acreedor(a) o deudor(a) de alguna de las personas interesadas en la actuación administrativa, su representante o apoderado(a), salvo cuando se trate de persona de derecho público, establecimiento de crédito o sociedad anónima. Que el cónyuge, compañero(a) permanente o alguno de los parientes dentro de los grados de consanguinidad o afinidad establecidos por la normatividad del servidor(a) público(a) o colaborador(a) del Estado, sea acreedor(a) o deudor(a) de alguna de las personas interesadas en la actuación administrativa, su representante o apoderado(a), salvo cuando se trate de persona de derecho público, establecimiento de crédito o sociedad anónima. |
| **10** | **Antiguo empleador.** | Que el servidor(a) público(a) o colaborador(a) del Estado, dentro del año anterior, haya tenido interés directo o haya actuado como representante, asesor(a), presidente(a), gerente(a), director(a), miembro(a) de Junta Directiva o socio(a) de gremio, sindicato, sociedad, asociación o grupo social o económico interesado(a) en el asunto objeto de definición. |
| **11** | **Lista de candidatos.** | Que el servidor(a) público(a) o colaborador(a) del Estado haya hecho parte de listas de candidatos a cuerpos colegiados de elección popular inscritas o integradas también por el interesado(a) en el período electoral coincidente con la actuación administrativa o en alguno de los dos períodos anteriores. |
| **12** | **Recomendación.** | Que el servidor(a) público(a) o colaborador(a) del Estado haya sido recomendado(a) por el interesado(a) en la actuación para llegar al cargo que ocupa o haya sido señalado por este como referencia con el mismo fin. |
| **13** | **Relación contractual o de negocios.** | Que alguno de los interesados(as) en la actuación administrativa sea representante, apoderado(a), dependiente, mandatario(a) o administrador(a) de los negocios del servidor(a) público(a) o colaborador(a) del Estado. |
| **14** | **Participación directa/asesoría de alguna de las partes interesadas.** | Que el servidor(a) público(a) o colaborador(a) del Estado hubiere participado en la expedición del acto enjuiciado, en la formación o celebración del contrato o en la ejecución del hecho u operación administrativa materia de la controversia. Que el cónyuge, compañero(a) o compañera permanente, o los parientes dentro de los grados de consanguinidad o afinidad establecidos por la normatividad tengan la calidad de asesores(as) o contratistas de alguna de las partes o de los terceros interesados vinculados al proceso, o tengan la condición de representantes legales o socios(as) mayoritarios(as) de una de las sociedades contratistas de alguna de las partes o de los terceros interesados. |
| **15** | **Participación en proceso arbitral respecto de cuyo laudo** | Que el(la) juez(a) hubiere intervenido en condición de árbitro(a), de parte, de tercero interesado(a), de apoderado(a), de testigo(a), de perito(a) o de agente del |

| ÍTEM | TIPOLOGÍA | DESCRIPCIÓN DE LA SITUACIÓN |
|---|---|---|
| | **se esté surtiendo recurso de anulación.** | Ministerio Público en el proceso arbitral respecto de cuyo laudo se esté surtiendo el correspondiente recurso de anulación ante la Jurisdicción de lo Contencioso Administrativo. Que el cónyuge, compañero(a) permanente, los parientes dentro de los grados de consanguinidad o afinidad establecidos por la normatividad del juez(a) hubieren intervenido en condición de árbitro(a), de parte, de tercero interesado, de apoderado(a), de testigo(a), de perito(a) o de agente del Ministerio Público en el proceso arbitral respecto de cuyo laudo se esté surtiendo el correspondiente recurso de anulación ante la Jurisdicción de lo Contencioso Administrativo. |
| **16** | **Parientes en una de las entidades públicas que concurran al respectivo proceso.** | Que el cónyuge, compañero(a) permanente, o alguno de los parientes del juez(a) dentro de los grados de consanguinidad o afinidad establecidos en la normatividad tengan la condición de servidores(as) públicos(as) o contratistas en los niveles directivos, asesor(a) o ejecutivo(a) en una de las entidades públicas que concurran al respectivo proceso en calidad de parte o de tercero interesado. Cuando el cónyuge, compañero(a) permanente, o alguno de los parientes dentro de los grados de consanguinidad o afinidad establecidos en la normatividad sean servidores(as) públicos(as) o contratistas en los niveles directivos, asesor(a) o ejecutivo(a) en una de las entidades públicas y que estos sean parte dentro del proceso. |
| **17** | **Dádivas** | Que el servidor(a) público(a) o colaborador(a) del Estado reciba o haya recibido dádivas, agasajos, regalos, favores o cualquier otra clase de beneficios incluyendo dinero. |
| **18** | **Responsables de la Evaluación de Desempeño.** | Los responsables de evaluar el desempeño laboral de los empleados(as) de carrera o en período de prueba cuando se encuentren vinculados(as) con estos por matrimonio o por unión permanente o tengan parentesco dentro de los grados de consanguinidad o afinidad establecidos en la normatividad o exista enemistad grave con el empleado(a) a evaluar o cuando exista cualquier causal de impedimento o hecho que afecte su objetividad. |

**Fuente:** Instructivo para la declaración y registro de conflictos de interés del Departamento Administrativo del Servicio Civil Distrital 2022.

### Identificar roles, funciones y procesos expuestos a riesgo

Una vez comprendidas las situaciones, la entidad debe identificar dónde es más probable que se presenten conflictos de interés. Esto implica un análisis práctico de:

- Los manuales de funciones y perfiles de cargo
- Los roles que participan en situaciones como:
  - evaluación
  - priorización
  - contratación
  - supervisión
  - toma de decisiones administrativas

No se debe limitar este análisis a niveles directivos. Muchos riesgos se materializan en niveles operativos donde existe capacidad de decisión o influencia.

Adicionalmente, se recomienda revisar los procesos y procedimientos institucionales para identificar puntos críticos, tales como:

- Definición de requisitos en contratación
- Evaluación de propuestas
- Asignación de beneficios o recursos
- Validación de información
- Supervisión de contratos

El resultado esperado de este ejercicio es un panorama claro de dónde pueden ocurrir conflictos de interés dentro de la entidad, estos son algunos ejemplos que se pueden identificar en procesos transversales y de apoyo a la gestión, sin embargo, cada entidad deberá ampliar este análisis a los procesos misionales propios de cada entidad y las eventualidades situaciones que presenten discrecionalidad por parte de los colaboradores públicos.

**Divulgar y socializar el procedimiento desde la realidad institucional**

El procedimiento debe ser divulgado de manera que los servidores y colaboradores lo reconozcan como una herramienta útil para su trabajo y no como un requisito adicional. Para ello, la socialización debe partir de situaciones reales de la entidad, utilizando ejemplos concretos que permitan entender cuándo se configura un conflicto de interés y qué se espera en cada caso.

Un aspecto fundamental en este proceso es desarrollar estrategias de cambio que permitan transformar la percepción frente al conflicto de interés. En estas situaciones existe la idea de que declarar un conflicto de interés puede generar consecuencias negativas o que implica reconocer una conducta indebida. Esta percepción debe ser abordada de manera directa y pedagógica.

Es importante transmitir un mensaje destacado: tener un conflicto de interés no es corrupción, ni es una falta; es una situación que puede presentarse en el ejercicio de la función pública. El riesgo real está en no declararlo o no gestionarlo adecuadamente.

En este sentido, la divulgación debe enfocarse en:

- Explicar que la declaración es un mecanismo de protección tanto para el servidor como para la entidad.
- Mostrar que declarar oportunamente permite tomar decisiones objetivas y evitar cuestionamientos posteriores.
- Generar confianza en el procedimiento, evitando que se perciba como un mecanismo sancionatorio.
- Promover una cultura en la que la transparencia sea vista como una práctica esperada y valorada.

Adicionalmente, se recomienda que las estrategias de socialización:

- Utilicen lenguaje sencillo y cercano
- Incluyan ejemplos propios de la entidad
- Diferencien situaciones según áreas o procesos
- Expliquen claramente qué ocurre después de declarar

La apropiación del procedimiento depende en gran medida de este paso. Sin comprensión y confianza en el proceso, incluso los mejores instrumentos tienden a no ser utilizados o a aplicarse de manera formal sin impacto real en la toma de decisiones.

**Definir un flujo de gestión claro, sencillo y con respaldo normativo**

El procedimiento debe estructurarse como una secuencia clara de pasos que permita gestionar adecuadamente las situaciones de conflicto de interés, garantizando decisiones objetivas y trazables. Este flujo debe estar alineado con lo establecido en la normativa colombiana, particularmente en materia de impedimentos y recusaciones.

De acuerdo con la Ley 1437 de 2011, los servidores públicos tienen la obligación de declararse impedidos cuando se encuentren incursos en alguna de las causales establecidas (art. 11), y cualquier interesado puede recusarlos cuando considere que existe una situación que afecta su imparcialidad (art. 12). Estas disposiciones constituyen la base jurídica para la gestión institucional del conflicto de interés.

A partir de este marco, el procedimiento debe contemplar los siguientes pasos:

*Tabla 2 Pasos para la gestión institucional del conflicto de interés.*

| Paso | Descripción | Actor responsable | Soporte normativo | Posible acción / resultado |
|---|---|---|---|---|
| **1. Identificación** | El servidor reconoce una situación que puede afectar su imparcialidad en el ejercicio de sus funciones. | Servidor público o contratista | Constitución Política de Colombia, art. 209 (principio de imparcialidad) | Reconocimiento del posible conflicto de interés |
| **2. Declaración de impedimento** | El servidor manifiesta la situación y se abstiene de continuar en la actuación hasta que se tome una decisión. | Servidor público | Ley 1437 de 2011, art. 11; Ley 1952 de 2019 | Registro del impedimento y suspensión de la actuación |
| **3. Recepción y análisis** | La autoridad competente evalúa si la situación configura una causal de impedimento. | Jefe inmediato o instancia designada | Ley 1437 de 2011, art. 11 | Determinación de existencia o no del conflicto |
| **4. Toma de decisión** | Se adopta una decisión frente al caso analizado. Puede incluir aceptar o rechazar el impedimento o resolver una recusación. | Autoridad competente | Ley 1437 de 2011, arts. 11 y 12 | - Aceptar impedimento- Rechazar impedimento- Reasignar funciones- Resolver recusación |

| Paso | Descripción | Actor responsable | Soporte normativo | Posible acción / resultado |
|---|---|---|---|---|
| **5. Registro y trazabilidad** | Se documenta la declaración, el análisis y la decisión adoptada para efectos de control y transparencia. | Área jurídica, talento humano o quien haga sus veces | Ley 1712 de 2014; Ley 594 de 2000 | Registro institucional del caso y archivo documental |
| **6. Seguimiento** | Se verifica el cumplimiento de la decisión y se identifican posibles situaciones asociadas. | Control interno o instancia responsable | Ley 87 de 1993 | Validación de cumplimiento y control del riesgo |

**Fuente:** Elaboración propia Dirección Distrital de Desarrollo Institucional.

**Importante:** La autoridad competente para decidir sobre impedimentos y recusaciones debe definirse de manera expresa por cada entidad de acuerdo con su estructura organizacional y competencias internas. Esta función puede recaer, según el caso, en el jefe inmediato, el superior jerárquico, la oficina jurídica, talento humano, comités institucionales o la instancia que haga sus veces. De conformidad con el artículo 12 de la Ley 1437 de 2011, cuando el servidor público no tenga superior jerárquico dentro de la entidad, la actuación deberá remitirse a la cabeza del respectivo sector administrativo y, a falta de este, al Procurador General de la Nación cuando se trate de autoridades nacionales, al Alcalde Mayor del Distrito Capital o al procurador regional en el caso de autoridades territoriales. La autoridad competente podrá aceptar o rechazar el impedimento y, de ser necesario, designar un funcionario ad hoc para conocer del asunto.

Finalmente, la gestión institucional de los conflictos de interés no debe limitarse al tratamiento individual de los casos reportados. La consolidación y análisis de las situaciones identificadas permite reconocer patrones, tipologías recurrentes, áreas críticas y posibles debilidades en los controles institucionales, generando insumos para el fortalecimiento del proceso y de la cultura de integridad al interior de las entidades.

Asimismo, cuando un conflicto de interés se materializa —es decir, cuando la situación afecta efectivamente la imparcialidad de una decisión o actuación administrativa— la entidad deberá activar las rutas correspondientes según la naturaleza del caso. Esto puede incluir acciones correctivas internas, como la revisión de actuaciones, la reasignación de funciones o el fortalecimiento de controles institucionales; así como actuaciones disciplinarias derivadas del incumplimiento del deber de declararse impedido. En particular, el artículo 44 de la Ley 1952 de 2019 establece la obligación de todo servidor público de declararse impedido cuando exista un interés particular y directo en una actuación, mientras que el artículo 72 de la misma ley tipifica como falta gravísima actuar u omitir pese a la existencia de causales de incompatibilidad, inhabilidad, impedimento o conflicto de interés establecidos en la Constitución o en la ley. En los casos que corresponda, la entidad también podrá realizar el traslado a autoridades competentes para el adelanto de actuaciones disciplinarias, fiscales o penales.

**Incorporar el SIDEAP como herramienta central de gestión**

El procedimiento para la gestión del conflicto de interés debe articularse con el Sistema de Información Distrital del Empleo y la Administración Pública (SIDEAP), como plataforma oficial para el registro, consulta y seguimiento de la información relacionada con los servidores públicos del Distrito.

El SIDEAP no debe entenderse únicamente como un repositorio de información, sino como una herramienta que permite dar soporte institucional a la gestión del conflicto de interés, facilitando la trazabilidad de las declaraciones y aportando insumos para la toma de decisiones.

En el marco del procedimiento, se recomienda incorporar de manera clara el uso de los siguientes módulos:

- **Conflicto de interés:** permite registrar las situaciones declaradas por los servidores públicos, facilitando su análisis y seguimiento institucional.
- **Bienes y rentas:** aporta información relevante para identificar posibles intereses económicos que puedan generar conflictos.
- **Personas Expuestas Políticamente (PEP):** permite reconocer condiciones de riesgo asociadas a roles o cargos con mayor nivel de exposición.

El procedimiento debe definir explícitamente:

- En qué momento se realiza el registro en SIDEAP
- Quién es responsable de diligenciar la información
- Cómo se utiliza la información registrada para la toma de decisiones
- Cómo se articula con el flujo de gestión del conflicto de interés

El procedimiento debe incorporar el uso del Sistema de Información Distrital del Empleo y la Administración Pública (SIDEAP) como herramienta central para la gestión del conflicto de interés, permitiendo el registro, consulta y seguimiento de la información relacionada con las declaraciones realizadas por los servidores públicos. En este sentido, el SIDEAP facilita la trazabilidad de las situaciones declaradas y aporta insumos para la toma de decisiones objetivas, en articulación con los procesos institucionales.[5]

Para su correcta implementación, la entidad debe orientar a los servidores sobre el uso del sistema, apoyándose en los instructivos dispuestos por el Departamento Administrativo del Servicio Civil Distrital (DASCD), los cuales explican de manera práctica cómo realizar el registro de conflictos de interés y su actualización[1]. Así mismo, el uso del SIDEAP debe enmarcarse en los lineamientos establecidos para la implementación del módulo de declaración de conflicto de interés en el Distrito Capital.[6]

**Seguimiento, gestión y toma de decisiones informadas**

[5] Departamento Administrativo del Servicio Civil Distrital (DASCD). *Instructivo de Declaración y Registro de Conflicto de Interés – SIDEAP*. Disponible en: https://www.serviciocivil.gov.co/tablero-de-control/info-importante-tablero-de-control/instructivo-de-declaracion-y-registro-de
[6] Departamento Administrativo del Servicio Civil Distrital (DASCD). *Circular Externa 020 de 2021,* "Implementación del módulo de declaración de conflicto de interés en el SIDEAP".

La gestión del conflicto de interés no finaliza con la declaración o el registro en el SIDEAP. Es fundamental que la entidad establezca mecanismos que permitan hacer seguimiento a las situaciones declaradas, verificar su adecuada gestión y utilizar esta información como insumo para la toma de decisiones institucionales.

En este sentido, el procedimiento debe contemplar acciones orientadas a:

- **Verificar el cumplimiento de las decisiones adoptadas**, asegurando que los impedimentos aceptados se materialicen efectivamente (por ejemplo, apartamiento de la actuación o reasignación de funciones).
- **Realizar seguimiento a los casos registrados**, identificando si existen situaciones recurrentes, patrones o áreas con mayor exposición al riesgo.
- **Analizar la información disponible en el SIDEAP**, integrándola con otros insumos institucionales como matrices de riesgo, procesos de control interno o reportes de gestión.
- **Generar alertas tempranas**, cuando se evidencien posibles concentraciones de decisiones, vínculos recurrentes o situaciones que puedan afectar la imparcialidad.

Adicionalmente, se recomienda que la entidad utilice esta información para fortalecer la gestión del riesgo, permitiendo:

- Incorporar el conflicto de interés como causa en la identificación de riesgos de integridad
- Ajustar controles en procesos críticos
- Orientar acciones de capacitación o intervención institucional

Este paso permite pasar de una gestión reactiva a un enfoque preventivo, en el que la información registrada no solo cumple una función de control, sino que se convierte en un insumo estratégico para garantizar la objetividad en la toma de decisiones y la prevalencia del interés general.

## Capítulo 2 Gestión del Riesgo de Lavado de activos (LA), financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP)

El Distrito Capital ha desarrollado un proceso sostenido de fortalecimiento de capacidades institucionales para la prevención y gestión de los riesgos asociados con el lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva, en adelante LA/FT/FP. Este proceso constituye un antecedente institucional que debe preservarse, actualizarse y articularse con los actuales referentes nacionales para la gestión integral del riesgo.[7]

En el ámbito distrital, la *Política Pública Distrital de Transparencia, Integridad y No Tolerancia con la Corrupción*, adoptada mediante el Documento CONPES D.C. 01 de 2019, estableció acciones

[7] Los principales hitos de este recorrido incluyen: Lineamiento para prevenir el lavado de activos y contra la financiación del terrorismo en las entidades distritales – Tomo I (noviembre de 2019); la Ruta metodológica para la implementación del SARLAFT (noviembre 2020) y el Documento Técnico de Adaptación de Medidas de Prevención y Mitigación del Riesgo de LA/FT (diciembre 2022). Este último contiene el marco conceptual, metodológico y las herramientas de apoyo (matrices de autodiagnóstico, formularios de reporte, señales de alerta, roles y responsabilidades) siendo el referente operativo complementario al presente lineamiento.

orientadas al fortalecimiento de las capacidades institucionales para prevenir y mitigar las prácticas que afectan la transparencia y la integridad. En desarrollo de esta política, la Circular 092 de 2020 de la Secretaría General proporcionó orientaciones para la implementación del Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo, SARLAFT, en las entidades distritales (Consejo Distrital de Política Económica y Social del Distrito Capital. (CONPES D.C.), 2019; Secretaría General de la Alcaldía Mayor de Bogotá D.C., 2020)

La presente estrategia actualiza, armoniza e integra estos antecedentes técnicos en el marco del Sistema de Gestión de Riesgos para la Integridad Pública, SIGRIP, de conformidad con la *Guía para la Gestión Integral del Riesgo en Entidades Públicas*, versión 7; la Ley 2195 de 2022; el Decreto 1122 de 2024; los Programas de Transparencia y Ética Pública, según corresponda; y la Política para la Gestión Integral de Riesgos de cada entidad. En este sentido, los desarrollos distritales previamente orientados a la implementación del SARLAFT, particularmente los derivados de la Circular 092 de 2020 de la Secretaría General de la Alcaldía Mayor de Bogotá D.C., se armonizan y articulan con el SIGRIP. En consecuencia, la gestión de los riesgos asociados al lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva, LA/FT/FP, se desarrollará en el marco del SIGRIP y de su articulación con el Programa de Transparencia y Ética Pública, sin perjuicio de los sistemas sectoriales, las obligaciones especiales y los regímenes de administración de riesgos aplicables a determinadas entidades distritales (DAFP, 2025; Ley 2195 de 2022, art. 31, par. 1; Decreto 1122 de 2024).

La Guía para la Gestión Integral del Riesgo en las Entidades Públicas, versión 7 incorpora el SIGRIP como un sistema orientado a prevenir, detectar y corregir los eventos que amenazan la integridad de las instituciones públicas. Su implementación articula la Política para la Gestión Integral de Riesgos, el mapa institucional de riesgos, la debida diligencia en el conocimiento de las contrapartes, la función de cumplimiento y las demás herramientas institucionales requeridas para la gestión de los riesgos para la integridad pública. Esta articulación debe considerar la naturaleza jurídica, la estructura, la misionalidad, las operaciones, el nivel de exposición al riesgo y el régimen aplicable a cada entidad (DAFP, 2025).

El LA/FT/FP constituye una amenaza para la integridad de las entidades públicas distritales, dado que las operaciones relacionadas con la administración de recursos públicos, la celebración de contratos o convenios, el otorgamiento de subsidios o beneficios, la recepción de donaciones, la realización de pagos y recaudos, la ejecución de programas sociales y otras relaciones con contrapartes pueden ser utilizadas para dar apariencia de legalidad a activos de origen ilícito o canalizar recursos hacia actividades terroristas o relacionadas con la proliferación de armas de destrucción masiva. Por esta razón, su gestión debe integrarse a la gestión institucional del riesgo y no desarrollarse como un sistema aislado (DAFP, 2025).

En el marco nacional, los artículos 323 y 345 de la Ley 599 de 2000 tipifican, respectivamente, el lavado de activos y la financiación del terrorismo y la administración de recursos relacionados con actividades terroristas. La Ley 526 de 1999 creó la Unidad de Información y Análisis Financiero, UIAF, como entidad técnica encargada de centralizar, sistematizar y analizar información relevante para la prevención y detección de estos fenómenos. A su vez, la Ley 1121 de 2006 fortaleció las medidas para su prevención y estableció, en su artículo 27, el deber de identificar plenamente a las personas naturales y jurídicas que suscriban contratos con el Estado, así como el origen de sus recursos (Ley 599 de 2000, arts. 323 y 345; Ley 526 de 1999, arts. 1, 3 y 4; Ley 1121 de 2006, art. 27).

La Ley 2195 de 2022 fortaleció la prevención, gestión y administración de los riesgos para la integridad pública y dispuso su incorporación en los Programas de Transparencia y Ética Pública.

El Decreto 1122 de 2024 reglamentó estos programas y reforzó su articulación con la gestión institucional del riesgo. De manera complementaria, el Documento CONPES 4042 de 2021 formuló la Política Nacional Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva, bajo un enfoque articulado y basado en riesgos. (Ley 2195 de 2022, art. 31; Decreto 1122 de 2024; Consejo Nacional de Política Económica y Social (CONPES), 2021).

En el Distrito Capital, el Acuerdo Distrital 1025 de 2026 estableció lineamientos para realizar el seguimiento y verificar la adopción de mecanismos de prevención y administración del riesgo de lavado de activos y financiación del terrorismo por parte de las entidades distritales. Este acuerdo refuerza la necesidad de contar con medidas institucionales documentadas, verificables y articuladas con la gestión del riesgo (Acuerdo Distrital 1025 de 2026).

En el ámbito internacional, las convenciones de Viena de 1988, Palermo de 2000 y el Convenio Internacional para la Represión de la Financiación del Terrorismo constituyen referentes para la prevención del lavado de activos, la delincuencia organizada transnacional y la financiación del terrorismo.[8]

Por su parte, las Recomendaciones del Grupo de Acción Financiera Internacional, GAFI, constituyen estándares internacionales para la prevención y gestión del LA/FT/FP. Su enfoque basado en riesgos implica identificar, comprender y evaluar la exposición de cada organización, y establecer medidas proporcionales a su naturaleza, operaciones, contrapartes, canales, jurisdicciones y capacidades institucionales. Estas recomendaciones constituyen referentes técnicos incorporados progresivamente al marco nacional mediante normas, políticas públicas, regímenes sectoriales y orientaciones institucionales (Grupo de Acción Financiera Internacional (GAFI), 2012, actualizado en 2026; CONPES, 2021).

En conjunto, estos antecedentes proporcionan el marco para que las entidades distritales gestionen los riesgos asociados con LA/FT/FP de manera integral, proporcional y articulada con su Política para la Gestión Integral de Riesgos, el SIGRIP, el Programa de Transparencia y Ética Pública y los sistemas sectoriales aplicables. El desarrollo completo de las disposiciones constitucionales, legales, reglamentarias, distritales y técnicas se encuentra en el **Anexo 1. Marco normativo**, que forma parte integral de la presente estrategia.

## 2.1. Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva (ALA/CFT/CFP)

Las entidades distritales, incorporarán dentro de su Política para la Gestión Integral de Riesgos lineamientos orientados a la prevención, detección, control y monitoreo de los riesgos asociados al lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva (LA/FT/FP), como parte de la gestión integral de los riesgos para la integridad pública.[9]

[8] Estos instrumentos fueron incorporados al ordenamiento colombiano mediante las leyes 67 de 1993, 800 de 2003 y 808 de 2003, respectivamente (Naciones Unidas, 1988, 1999, 2000; Ley 67 de 1993; Ley 800 de 2003; Ley 808 de 2003)

[9] Adaptado de los numerales 6.3, 6.3.5, 6.3.5.2, 6.3.5.3 y 6.3.5.4 del Capítulo VI "Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP)" de la Guía para la Gestión Integral del Riesgo en las Entidades Públicas, versión 7 del Departamento Administrativo de la Función Pública

La gestión de estos riesgos deberá desarrollarse de manera articulada con los demás componentes del SIGRIP, considerando que la Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva ALA/CFT/CFP constituye una de las herramientas de gestión previstas en dicho sistema y complementa los mecanismos institucionales relacionados con la gestión integral de riesgos, la debida diligencia en el conocimiento de las contrapartes, la función de cumplimiento y el procedimiento para el Reporte de Operaciones Sospechosas.

En este contexto, cada entidad formulará, adoptará e implementará una Política ALA/CFT/CFP que refleje el compromiso de la Alta Dirección y de las instancias de dirección o gobierno que existan en la entidad con la prevención y mitigación de los riesgos asociados al LA/FT/FP, contribuyendo al fortalecimiento de la integridad pública.

La política deberá contemplar lineamientos aplicables a los procesos, procedimientos, servidores públicos, trabajadores oficiales, contratistas, miembros de órganos de dirección y demás contrapartes con las que la entidad mantenga interacciones, relaciones institucionales, administrativas, contractuales, financieras, operativas o de cualquier otra naturaleza, en el marco de sus competencias y de conformidad con la normatividad vigente.

### 2.1.1. Declaración de la Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva (ALA/CFT/CFP)

De conformidad con lo previsto en el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), la Política ALA/CFT/CFP constituye una herramienta institucional orientada a fortalecer la prevención, detección, control y monitoreo de los riesgos asociados al LA/FT/FP, contribuyendo a la protección de la integridad pública y al cumplimiento de la normatividad aplicable.[10]

En este apartado se definen los elementos mínimos que deberá contener esta política, los cuales constituyen el estándar mínimo esperado para las entidades distritales y podrán ser desarrollados o complementados atendiendo su naturaleza jurídica, contexto institucional, estructura organizacional y nivel de madurez en la gestión de riesgos.

a. **Elementos mínimos de la Política ALA/CFT/CFP**

La política deberá contemplar, como mínimo:

a) El compromiso expreso de la Alta Dirección o la que haga sus veces, con la prevención y mitigación de los riesgos asociados al LA/FT/FP.
b) La prohibición y rechazo de cualquier práctica asociada al LA/FT/FP.
c) El compromiso institucional de cumplir con la normatividad aplicable en materia ALA/CFT/CFP.
d) La obligación de actuar con debida diligencia en el conocimiento de las contrapartes.
e) La promoción del reporte de actividades u operaciones asociadas a las señales de alerta definidas por la entidad.
f) La promoción de una cultura de reporte libre de represalias y el tratamiento confidencial de la información correspondiente.

[10] Adaptado de los numerales 6.3.5.4 literal a), 6.3.5.2, 6.3.5.3 y 6.3.6 de la misma guía.

g) La incorporación de pautas generales de comportamiento orientadas a fortalecer la integridad, la transparencia y la legalidad en las actuaciones institucionales.
h) La revisión y actualización de la política cuando se presenten cambios normativos, institucionales, operativos o en el nivel de exposición a los riesgos asociados al LA/FT/FP, de acuerdo con las condiciones y mecanismos definidos por cada entidad.
i) La referencia a las consecuencias asociadas al incumplimiento de la política, de conformidad con el ordenamiento jurídico vigente y las competencias de las autoridades correspondientes.

A continuación, se presenta un texto orientador que podrá ser adaptado por cada entidad, conservando los elementos mínimos anteriormente descritos.

b. **Declaración de política**

La entidad *(incorpore el nombre de la entidad)* adopta la presente Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva (ALA/CFT/CFP), mediante la cual manifiesta de manera expresa el compromiso de la Alta Dirección y de las instancias de dirección y gobierno institucional con el fortalecimiento de una cultura organizacional orientada a la prevención, detección, control y monitoreo de los riesgos asociados al lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva.

La entidad *prohíbe y rechaza* cualquier práctica que pueda facilitar o favorecer actividades relacionadas con el lavado de activos, la financiación del terrorismo o la financiación de la proliferación de armas de destrucción masiva, y desarrollará sus actuaciones de conformidad con la normatividad vigente aplicable en la materia, promoviendo su cumplimiento en el desarrollo de todas las actividades institucionales.

Así mismo, la entidad *actuará con debida diligencia en el conocimiento de sus contrapartes*, mediante la aplicación de procedimientos orientados a la obtención, validación y análisis de información relevante para la gestión de riesgos asociados al LA/FT/FP, de conformidad con los lineamientos institucionales que se adopten para tal fin. Igualmente, promoverá mecanismos para la identificación y análisis de señales de alerta y el reporte de actividades u operaciones que deban ser objeto de evaluación conforme a los procedimientos institucionales establecidos.

La entidad promoverá una cultura institucional orientada al reporte oportuno de situaciones asociadas a los riesgos LA/FT/FP, garantizando la confidencialidad de la información y promoviendo que dicho reporte se realice sin temor a represalias.

Los servidores públicos, trabajadores oficiales, contratistas y demás personas que participen en el desarrollo de actividades institucionales deberán actuar con integridad, transparencia, diligencia y responsabilidad, observando los lineamientos, procedimientos y controles establecidos por la entidad para la gestión de los riesgos asociados al LA/FT/FP.

**c. Pautas de comportamiento**

En desarrollo de la presente política, los destinatarios deberán:

- Conocer y aplicar las disposiciones, lineamientos, procedimientos y controles definidos por la entidad para la gestión de riesgos asociados al LA/FT/FP.
- Actuar de manera diligente en el desarrollo de las actividades relacionadas con sus funciones, obligaciones o responsabilidades.
- Atender los procedimientos y mecanismos definidos por la entidad para el conocimiento de las contrapartes, suministrando la información requerida y apoyando las actividades

de validación, verificación y análisis que resulten aplicables de acuerdo con sus funciones o responsabilidades.

- Informar a la instancia o dependencia competente aquellas actividades u operaciones que, de acuerdo con los criterios y señales de alerta definidos por la entidad, requieran análisis o verificación.
- Suministrar la información requerida para el desarrollo de actividades de análisis, monitoreo o gestión de riesgos asociados al LA/FT/FP.
- Preservar la confidencialidad de la información relacionada con alertas, reportes o análisis que se adelanten en el marco de esta política.
- Participar en las actividades de capacitación, sensibilización y fortalecimiento institucional que promueva la entidad en esta materia.

**d. Prohibiciones**

Los destinatarios de la presente política se abstendrán de:

- Realizar, facilitar, promover u ocultar actividades asociadas al LA/FT/FP.
- Omitir u obstaculizar injustificadamente las actividades de identificación, análisis, monitoreo o reporte asociadas a la gestión de estos riesgos.
- Utilizar su posición o acceso a información para favorecer intereses particulares en contravía de los principios de integridad y legalidad.
- Ocultar, encubrir, simular o desnaturalizar operaciones con el propósito de evadir los controles establecidos por la entidad.
- Divulgar información relacionada con alertas, reportes o análisis a personas no autorizadas, salvo los casos permitidos por la ley.

**e. Enfoque institucional frente a la materialización del riesgo**

La gestión de los riesgos asociados al LA/FT/FP tiene como propósito fortalecer la capacidad institucional para identificar, medir, controlar y monitorear situaciones que puedan afectar la integridad pública, promoviendo acciones orientadas a prevenir, detectar y corregir oportunamente eventos de riesgo.

Las actuaciones desarrolladas en el marco de esta política tienen carácter preventivo y de gestión del riesgo. En consecuencia, la identificación, análisis, monitoreo o reporte de situaciones asociadas al LA/FT/FP no constituyen, por sí mismos, juicios de responsabilidad ni implican la imposición de sanciones, las cuales corresponden a las autoridades competentes de conformidad con el ordenamiento jurídico vigente

Ante escenarios de materialización de riesgos, la entidad promoverá la adopción de acciones orientadas a gestionar sus efectos y contribuir a la continuidad del servicio y de la operación institucional, sin perjuicio de las actuaciones que correspondan a las autoridades competentes en ejercicio de sus funciones.

**f. Consecuencias del incumplimiento**

El incumplimiento de los lineamientos, procedimientos o controles asociados a la gestión de riesgos ALA/CFT/CFP será puesto en conocimiento de las instancias o autoridades competentes cuando los hechos puedan tener relevancia administrativa, disciplinaria, contractual, fiscal, penal o de cualquier otra naturaleza prevista en la normatividad vigente.

La determinación de responsabilidades corresponderá exclusivamente a las autoridades competentes, con observancia del debido proceso, el derecho de defensa y las demás garantías constitucionales y legales aplicables.

## 2.2. ¿Cómo diferenciar las amenazas LA/FT/FP en la gestión institucional?

Aunque el lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva LA/FT/FP pueden involucrar operaciones, contrapartes o canales similares, se diferencian por el origen, el destino o el uso de los recursos. Estas diferencias permiten identificar los escenarios de riesgo y definir las medidas de prevención, monitoreo y control.[11]

*Ilustración 1 Diferencias en el análisis de riesgos asociados a LA/FT/FP*




Fuente: Elaboración propia a partir de *"Lo que debe saber sobre el lavado de activos y la financiación del terrorismo" (UIAF, 2014).*

En el Distrito Capital, los riesgos asociados al LA/FT/FP pueden presentarse en contratos, convenios, subsidios, donaciones, pagos, recaudos, transferencias, gestión de bienes y otras operaciones o transacciones que involucren intercambio de bienes y servicios en el marco de una relación con una contraparte. Sin embargo, no todas las entidades están expuestas de la misma manera, pues los escenarios de riesgo dependen de sus funciones, procesos, operaciones y tipos de contrapartes.

Por esta razón, cada entidad analizará en qué actividades o momentos de sus procesos existe la posibilidad de que sus operaciones sean utilizadas para:

- Dar apariencia de legalidad a activos de origen ilícito.
- Canalizar o destinar recursos hacia actividades terroristas.
- Facilitar la financiación de actividades relacionadas con la proliferación de armas de destrucción masiva.

Este análisis permitirá orientar el conocimiento de las contrapartes, la aplicación de la debida diligencia[12], la identificación y documentación de señales de alerta, el diseño de controles y el monitoreo de las operaciones o transacciones. La identificación de una etapa o forma de manifestación de LA/FT/FP constituye una señal para realizar un análisis más detallado. Por sí sola, no permite concluir que la operación sea sospechosa, que el riesgo se haya materializado o que se haya cometido una conducta contraría a la ley.

[11] Para las definiciones de lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva, así como para la explicación de sus etapas o formas de manifestación, véase el marco conceptual de la presente estrategia.
[12] Ver capítulo 4 Debida diligencia en el conocimiento de las contrapartes

## 2.3. El LA/FT/FP como amenaza a la Integridad Pública

El LA/FT/FP constituye una amenaza para la integridad pública porque las entidades pueden ser utilizadas para dar apariencia de legalidad a activos de origen ilícito o para canalizar recursos hacia actividades terroristas o relacionadas con la proliferación de armas de destrucción masiva. Esta exposición puede relacionarse con otras amenazas, como la corrupción, el fraude o el soborno, por lo que su gestión debe articularse con el SIGRIP y con la Política para la Gestión Integral de Riesgos de cada entidad.

La exposición al LA/FT/FP puede presentarse aun cuando no exista una actuación indebida de un servidor o colaborador. Por esta razón, su identificación debe centrarse en las operaciones o actividades de los procesos en las que la entidad recibe, entrega, administra, transfiere o autoriza recursos, bienes o servicios en el marco de una relación con una contraparte.

**a. ¿Cómo aplicar la metodología de gestión del riesgo a LA/FT/FP?**

La identificación, descripción, análisis y valoración de los riesgos asociados con LA/FT/FP se realizará mediante la metodología general definida en la Política para la Gestión Integral de Riesgos de cada entidad y las orientaciones de la *Guía para la Gestión Integral del Riesgo en Entidades Públicas*, versión 7. Estos riesgos se incorporan al mapa institucional y no requieren una metodología ni una matriz independiente. (DAFP, 2025).

Para aplicar esta metodología, la entidad identificará las operaciones o actividades de sus procesos en las que se intercambian recursos, bienes o servicios con una contraparte. Estas operaciones constituyen los puntos de riesgo que deben analizarse.

Como parte de este análisis, la entidad considerará los factores de riesgo asociados a las contrapartes, los productos o servicios, los canales y las jurisdicciones presentes en sus operaciones. Estos factores podrán segmentarse mediante la conformación de grupos con características similares, teniendo en cuenta la naturaleza, el contexto, la disponibilidad y calidad de la información y las capacidades institucionales. La segmentación permitirá conocer de manera diferenciada la exposición al riesgo y servirá como insumo para definir medidas de debida diligencia, criterios de monitoreo y señales de alerta acordes con las características de las operaciones y contrapartes.

La identificación y descripción del riesgo puede desarrollarse a partir de cuatro elementos:

1. **Punto de riesgo:** operación o actividad del proceso en la que existe intercambio de recursos, bienes o servicios con una contraparte.
2. **Impacto:** posible afectación económica, reputacional, legal, operativa o de contagio para la entidad.
3. **Causa inmediata:** posibilidad de que la entidad sea utilizada para dar apariencia de legalidad a activos provenientes de actividades ilícitas o para canalizar recursos hacia actividades terroristas o relacionadas con la proliferación de armas de destrucción masiva.
4. **Causa raíz:** operación o transacción en la que existe la vulnerabilidad o exposición al riesgo.

*Ilustración 2 De la identificación a la descripción de los riesgos asociados a LA/FT/FP*




Fuente: Elaboración propia con base en la *Guía para la Gestión Integral del Riesgo en Entidades Públicas*, versión 7.

En cuanto a la descripción del riesgo, esta inicia con la expresión **"posibilidad de"** e identifica el impacto, la causa inmediata y la causa raíz.

***Ejemplo aplicado***

*Posibilidad de afectación económica y reputacional por el uso de la entidad para dar apariencia de legalidad a activos de origen ilícito, causado por deficiencias en la identificación y verificación de los beneficiarios finales durante la vinculación de contrapartes en los procesos de contratación directa.*

*Ilustración 3 Elementos de la descripción del riesgo*




Fuente: Ejemplo elaborado con base en la estructura para la descripción de riesgos establecida en la *Guía para la Gestión Integral del Riesgo en Entidades Públicas*, versión 7.

El ejemplo permite identificar la operación en la que puede presentarse la exposición, es decir, la forma en que podría utilizarse la entidad y la circunstancia que origina el riesgo.

Una vez identificado y descrito el riesgo, el análisis de probabilidad e impacto, el diseño y valoración de los controles, la determinación del riesgo residual y su tratamiento se realizarán

conforme a la Política para la Gestión Integral de Riesgos de la entidad y a la metodología general establecida en la *Guía para la Gestión Integral del Riesgo en Entidades Públicas*, versión 7.

Los elementos del SIGRIP, como la debida diligencia en el conocimiento de las contrapartes, la función de cumplimiento y las herramientas institucionales de gestión, podrán contribuir al diseño de los controles aplicables a los riesgos identificados, de acuerdo con las características y el nivel de exposición de cada entidad.

Una vez incorporado el riesgo al mapa institucional, los cinco pasos que se presentan a continuación facilitan su gestión práctica antes, durante y después de las operaciones, transacciones o relaciones con las contrapartes.

### b. Cinco pasos orientadores para la gestión de riesgos asociados a LA/FT/FP

La gestión de riesgos asociados al LA/FT/FP se materializa en decisiones y actuaciones concretas que los servidores o colaboradores de la entidad deben adoptar en diferentes momentos de su gestión.

Con el propósito de facilitar la comprensión y aplicación práctica de esta estrategia, se presentan cinco pasos orientadores dirigidos a los líderes de proceso y demás servidores o colaboradores de la entidad, con el fin de fortalecer la identificación, prevención y gestión de riesgos asociados a LA/FT/FP antes, durante y después de la interacción u operación con una contraparte.

Estos cinco pasos aplican la lógica de gestión de riesgos prevista en *Guía para la Gestión Integral del Riesgo en Entidades Públicas*, versión 7, para la amenaza de LA/FT/FP. Su contenido desarrolla aspectos propios de este componente, como el conocimiento y la segmentación de contrapartes, la identificación del beneficiario final, la debida diligencia, las señales de alerta, las operaciones inusuales y el reporte de operaciones sospechosas ante la UIAF; por ello, no se extienden de manera automática a las amenazas de fraude, soborno, corrupción e inadecuada gestión del conflicto de interés, las cuales aplican los instrumentos y procedimientos que correspondan a su naturaleza.

Cada paso incorpora ejemplos aplicados al contexto distrital, orientados a facilitar el reconocimiento de situaciones de riesgo en escenarios propios de la gestión pública, promoviendo así una gestión preventiva, articulada y basada en riesgos.

**PASO 1 ¿Dónde está mi riesgo?**

Identifique las operaciones vulnerables de su entidad, debido a que el riesgo asociado a LA/FT/FP no existe en toda la entidad por igual. Existe en los momentos concretos en que su entidad intercambia recursos con una contraparte. Antes de cualquier otra acción, la entidad debe identificar cuáles son esas operaciones en sus procesos.

***La pregunta que debe hacerse es:*** ¿en qué momentos de mi operación hay una transacción u operación de entrega de bienes o servicios entre mi entidad y un tercero?

***Ejemplos en el contexto distrital:***

- ✓ Una entidad que administra subsidios de vivienda tiene su mayor exposición en el momento del desembolso a los beneficiarios y en la verificación de los requisitos de quienes los solicitan, no en la elaboración interna de los informes de gestión.

- ✓ Una entidad que contrata servicios de mantenimiento de obras tiene su mayor exposición en el proceso de selección del contratista, en los pagos por avance y en la verificación de la ejecución contractual.
- ✓ Una entidad que otorga licencias de construcción tiene su mayor exposición en la revisión de la documentación aportada por el solicitante y en la verificación de la titularidad real del predio.

***Acción concreta:*** Revise los procesos de su entidad e identifique todas las actividades que implican un pago, un recaudo, la entrega de un bien o servicio, o la habilitación de un tercero para actuar. Esas son sus operaciones vulnerables y son el punto de partida del mapa de riesgos asociados a LA/FT/FP.

**PASO 2 ¿Quién me preocupa?**

Clasifique sus contrapartes según el nivel de riesgo que representan, debido a que no todas las contrapartes representan el mismo nivel de riesgo. Una empresa con años de relación con la entidad, con información pública disponible y con antecedentes verificables no es igual que una empresa recién constituida, con estructura de propiedad opaca, que ofrece precios significativamente por debajo del mercado.

***La pregunta que debe hacerse es***: ¿qué sé realmente de con quién estoy operando?

***Ejemplos en el contexto distrital:***

- ✓ Una organización social que recibe recursos distritales para atender población vulnerable y cuyos beneficiarios finales no están claramente identificados, representa un nivel de riesgo mayor que una entidad pública con la que se suscribe un convenio interadministrativo.
- ✓ Un proveedor de servicios tecnológicos registrado recientemente, cuyo representante legal figura en una jurisdicción de riesgo, requiere una debida diligencia más exigente que un proveedor con años de contratación con múltiples entidades del Estado.

**Nota:** Identificar una señal de alerta o clasificar una contraparte como de mayor riesgo no implica necesariamente que la entidad deba terminar la relación. En muchas actuaciones propias de la gestión pública, como el recaudo de impuestos, la prestación de servicios públicos o la atención de trámites y solicitudes, la entidad debe continuar ejerciendo sus funciones. En estos casos, el objetivo de la gestión del riesgo asociado a LA/FT/FP es aumentar los controles, hacer seguimiento a las operaciones y documentar adecuadamente las situaciones identificadas, más no restringir derechos o incumplir obligaciones propias de la entidad.

***Acción concreta:*** Agrupe sus contrapartes habituales según características comunes tipo de persona (natural o jurídica), antigüedad, sector, nivel de información disponible, origen de los recursos que utilizan y asigne un nivel de riesgo a cada grupo. Esa es su segmentación básica, y de ella derivan sus señales de alerta propias.

Los resultados de esta segmentación servirán como referencia para reconocer los comportamientos esperados de las contrapartes y de sus operaciones. A partir de estos resultados, la entidad podrá identificar variaciones o situaciones que se aparten de los patrones observados y definir las señales de alerta que requieran análisis. La segmentación no determina por sí misma que una operación sea inusual o sospechosa, sino que proporciona criterios para orientar su monitoreo y evaluación.

**PASO 3 ¿Qué hago antes?**

Aplique debida diligencia proporcional al nivel de riesgo antes de iniciar la relación, debido a que el momento más importante de la gestión del riesgo asociado a LA/FT/FP es antes de que la operación ocurra. Una vez el dinero ha sido transferido o el contrato está en ejecución, el margen de acción se reduce.

***La pregunta que debe hacerse es:*** ¿qué necesito verificar antes de proceder, y cuánto necesito verificar según el riesgo que representa esta contraparte?

El enfoque basado en riesgos implica que no se aplica el mismo nivel de verificación a todas las contrapartes.

***Ejemplos en el contexto distrital:***

- ✓ Para una contratación directa de bajo monto con un proveedor conocido y con historial en la entidad, la debida diligencia simplificada puede ser suficiente: consulta a listas vinculantes y restrictivas, verificación de existencia legal y revisión de antecedentes en las bases de datos obligatorias.
- ✓ Para un convenio con una organización no gubernamental que recibirá recursos distritales para operar en zonas con presencia de grupos al margen de la ley, la debida diligencia ampliada es indispensable: verificación de beneficiarios finales, análisis de la fuente de sus recursos y revisión de su estructura directiva.

***Acción concreta:*** Incorpore en los procedimientos de cada proceso con exposición al riesgo un punto de control explícito de debida diligencia antes de proceder con la operación, con el nivel de exigencia definido según el riesgo de la contraparte.

**PASO 4 ¿Qué hago durante?**

Monitoree señales de alerta a lo largo de la operación, puesto que la debida diligencia previa no elimina el riesgo; lo reduce. Durante la ejecución de la relación pueden aparecer situaciones que no estaban presentes al inicio y que cambian el perfil de riesgo de la contraparte. El monitoreo continuo es lo que permite detectarlas a tiempo.

***La pregunta que debe hacerse es***: ¿está ocurriendo algo que no corresponde al comportamiento esperado de esta contraparte?

*A manera de ejemplo, pueden constituir señales de alerta:* pagos solicitados a cuentas de terceros no vinculados con el contrato; cambios frecuentes e injustificados en la representación, el domicilio o las cuentas bancarias de la contraparte; operaciones cuyo monto o frecuencia no guarda relación con la actividad o el objeto contractual; el fraccionamiento injustificado de pagos; o la negativa a suministrar información que razonablemente debería estar disponible. Estos ejemplos son orientadores y no taxativos; una señal de alerta no implica, por sí sola, la existencia de una operación inusual, sino la necesidad de analizarla.

***Acción concreta:*** identifique, para cada proceso con exposición al riesgo, las señales de alerta pertinentes, construidas a partir del conocimiento real de cómo operan sus contrapartes habituales. Para ello podrá apoyarse en los ejemplos y escenarios contenidos en la *Caja de Herramientas para la Prevención de Riesgos de LA/FT/FPADM, versión 2.0,* elaborada por la Secretaría General de la Alcaldía Mayor de Bogotá con el apoyo de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), disponible en el ***Anexo 4 La Caja de Herramientas***

***para la Prevención de Riesgos de LA/FT/FPADM V 2.0.*** Las señales identificadas se documentarán y mantendrán actualizadas, de manera que sirvan de insumo para el monitoreo y la gestión de los riesgos de LA/FT/FP. Cuando una señal se active, el líder del proceso reportará al responsable de la función de cumplimiento, sin investigarla por su cuenta.

**PASO 5 ¿Qué hago si detecto algo?**

Reporte la situación por el canal definido por la entidad y aplique la ruta establecida en el numeral 2.5 *"Procedimiento para el Reporte de Operaciones Sospechosas"* de este documento, la cual comprende las acciones y responsables para la identificación de la señal de alerta, el reporte interno, el análisis por la función de cumplimiento y, cuando corresponda, el reporte ante las autoridades competentes; detectar una situación inusual significa que hay algo que no corresponde al comportamiento esperado de una contraparte y que merece análisis.

***La pregunta que debe hacerse es:*** ¿esto es inusual o es sospechoso, y qué hago en cada caso?

**La diferencia práctica:**

- Una *operación inusual*: es aquella que se sale del patrón normal de la contraparte, pero puede tener una explicación razonable. El líder de proceso la reporta al responsable de la función de cumplimiento, quien la analiza.
- Una *operación sospechosa*: es aquella que, tras el análisis, no tiene una explicación razonable que justifique su carácter atípico. El responsable de la función de cumplimiento la reporta ante la UIAF a través del SIREL incluso si la operación fue intentada y no se consumó, dado que el reporte de las operaciones intentadas procederá cuando reúna elementos objetivos que permitan calificarla como sospechosa y la entidad deba reportarla conforme a su régimen y calidad de reportante.

**Ejemplo de la ruta completa:**

- ✓ Durante la ejecución de un contrato, el supervisor identifica una situación que no corresponde al comportamiento esperado de la contraparte, evidenciando inconsistencias entre los soportes presentados y la ejecución del contrato. Ante esta situación, remite el caso al responsable de la función de cumplimiento para su análisis.
  El responsable solicita información adicional y revisa la documentación disponible. Como resultado del análisis, concluye que las inconsistencias identificadas no cuentan con una justificación razonable y podrían constituir una operación sospechosa (ROS). En consecuencia, procede a elaborar el ROS y a realizar el reporte correspondiente ante la UIAF a través del Sistema de Reporte en Línea (SIREL).
  Posteriormente, el caso sirve como insumo para fortalecer la gestión del riesgo institucional, actualizando las señales de alerta, ajustando controles y fortaleciendo las actividades de monitoreo asociadas al proceso correspondiente.

Lo que no debe hacer un el servidor o colaborador de la entidad cuando detecta una situación inusual es investigar por su cuenta, confrontar directamente a la contraparte sobre sus sospechas, o abstenerse de reportar por temor a equivocarse. El reporte de buena fe está protegido y no genera responsabilidad.

***Acción concreta:*** Asegúrese de que todos los líderes de proceso conozcan la ruta:

*Ilustración 4 Ruta completa para un reporte de operación sospechosa (ROS)*




Fuente: Elaboración propia con base en (Ley 526, 1999; Ley 2195, 2022; Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7).

**Nota:** Para el detalle de responsables y actuaciones, aplique el procedimiento del numeral 2.5 *"Procedimiento para el Reporte de Operaciones Sospechosas".*

## 2.4. Articulación con los demás elementos del SIGRIP.

La gestión del riesgo asociado a LA/FT/FP se articula de manera integral con la Política para la Gestión Integral de Riesgos, el Programa de Transparencia y Ética Pública PTEP, la debida diligencia, la función de cumplimiento, el esquema de líneas de aseguramiento y los procesos institucionales.

En primer lugar, la debida diligencia respecto de las contrapartes constituye un mecanismo de carácter preventivo, en tanto el conocimiento suficiente, oportuno y verificable de estas incluyendo su actividad económica real, el origen de los recursos y la identificación de los beneficiarios finales, permite reducir de manera significativa los niveles de exposición al riesgo de la entidad. En este sentido, los resultados derivados de los procesos de debida diligencia retroalimentan de forma permanente el análisis y la gestión del riesgo, estableciéndose una relación bidireccional entre ambos.

En segundo lugar, la función de cumplimiento desempeña un papel articulador dentro del sistema, en la medida en que define los criterios técnicos para la identificación de operaciones inusuales y sospechosas, recibe y evalúa los reportes internos remitidos por los líderes de los procesos y, conforme a las disposiciones normativas vigentes, adelanta el reporte externo ante la Unidad de Información y Análisis Financiero (UIAF), la Fiscalía General de la Nación u otras autoridades competentes cuando corresponda, a través del procedimiento establecido para el reporte de operación sospechosa (ROS).

La articulación no implica que todas las amenazas cuenten con los mismos factores, procedimientos, canales de reporte o consecuencias. Cada componente conservará los criterios técnicos propios de su naturaleza de conformidad con la *Guía para la Gestión Integral del Riesgo en Entidades Públicas*, versión 7.

## 2.5. Procedimiento para el Reporte de Operaciones Sospechosas

### 2.5.1. Contexto Normativo y alcance del componente

La identificación, análisis y reporte de operaciones sospechosas constituye uno de los principales mecanismos de prevención y detección del LA/FT/FP. Su finalidad es permitir que las entidades identifiquen oportunamente situaciones que, por sus características, cuantía, frecuencia o falta de justificación aparente, puedan estar asociadas con actividades de carácter ilícito y deban ser puestas en conocimiento de las autoridades competentes.

En Colombia, este mecanismo tiene como antecedente la creación de la Unidad de Información y Análisis Financiero (UIAF) mediante la Ley 526 de 1999, entidad responsable de centralizar, analizar y transmitir información para la prevención y detección de actividades relacionadas con el LA/FT (Ley 526, art.9 , 1999). A su vez, el artículo 42 de la Ley 190 de 1995 establece que el reporte de operación sospechosa (ROS) no constituye denuncia penal, tienen carácter reservado y no generan responsabilidad para la entidad reportante, ni para quienes participen en su detección o reporte, siempre que se actúe de buena fe (Ley 190, 1995, art. 42*).*

La confidencialidad del Reporte de Operación Sospechosa (ROS) se encuentra amparada por la reserva legal aplicable a la información que recauda y produce la UIAF, de conformidad con el artículo 9º de la Ley 526 de 1999, modificado por el artículo 34 de la Ley 1621 de 2013. En concordancia con este régimen, el acceso, uso y circulación de dicha información se encuentran restringidos a las autoridades competentes y a las finalidades legalmente previstas.

Posteriormente, la Ley 1121 de 2006, en su artículo 27, incorporó obligaciones específicas relacionadas con la identificación y verificación de contrapartes, especialmente en el ámbito de la contratación estatal, como parte de las medidas orientadas a la prevención del LA/FT (Ley 1121 de 2006, art. 27)

En el ámbito distrital, la gestión del riesgo asociado a LA/FT/FP ha sido desarrollada mediante diversos instrumentos técnicos expedidos por la Secretaría General de la Alcaldía Mayor de Bogotá entre 2020 y 2022, orientados a fortalecer la implementación del SARLAFT, el conocimiento de contrapartes, la identificación de señales de alerta, el reporte de operaciones sospechosas y la gestión integral de estos riesgos en las entidades distritales.[13]

La Ley 2195 de 2022 fortaleció dichas obligaciones en el sector público. En particular su artículo 31 modificó el artículo 73 de la Ley 1474 de 2011 estableciendo que cada entidad del orden nacional, departamental y municipal, cualquiera que sea su régimen de contratación deberá implementar un Programa de Transparencia y Ética Pública (PTEP). El literal b) de la disposición incluyó, entre los contenidos de dicho programa, la prevención, gestión y administración de los riesgos de LA/FT/FP, así como los reportes de operaciones sospechosas a la UIAF, las consultas en listas restrictivas y las demás medidas específicas que defina el Gobierno. (Ley 2195 , 2022)

En consecuencia, las entidades distritales de naturaleza pública que deban reportar directamente a la UIAF y no cuenten con un régimen especial de reporte verificarán si les corresponde realizar

[13] Entre estos instrumentos se encuentran la Circular 092 de 2020, la Ruta Metodológica para la Implementación del SARLAFT en las Entidades Distritales (2020), el Lineamiento para la Implementación del SARLAFT en las Entidades del Distrito (2021) y el Documento Técnico de Adaptación de Medidas de Prevención y Mitigación del Riesgo de LA/FT en las Entidades del Distrito Capital (2022).

sus reportes en SIREL a través del sector Ley 2195 de 2022. Si la entidad está sometida a un régimen especial de vigilancia, regulación o supervisión que establezca condiciones propias de reporte, aplicará las instrucciones correspondientes a ese sector. En caso de duda, consultará a la UIAF sobre cuál es el sector de reporte que le resulta aplicable. Los tipos de reporte, su periodicidad, los plazos y las demás condiciones para su presentación serán los establecidos en las disposiciones, anexos técnicos e instructivos vigentes de la UIAF. (Unidad de Análisis Financiero - UIAF, 2025)

En desarrollo de lo anterior, la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7, en el marco del SIGRIP, establece la necesidad de contar con procedimientos internos para la identificación de operaciones inusuales, la definición de señales de alerta, el análisis por parte de la función de cumplimiento y el reporte a la UIAF u otras autoridades competentes cuando se determine la existencia de una operación sospechosa (Departamento Administrativo de la Función Pública, 2025)

A nivel operativo, el Documento Técnico Distrital de LA/FT (2022) y la *Caja de Herramientas para la Prevención de Riesgos de LA/FT/FPADM – Versión 2.0* constituyen referentes complementarios para la aplicación práctica de estas disposiciones, particularmente en lo relacionado con la identificación, análisis y reporte de operaciones inusuales y sospechosas (Documento Técnico de Adaptación Medidas de Prevención y Mitigacion - SARLAFT, 2022).

### 2.5.2. ¿Qué se espera del componente en el SIGRIP Distrital?

En el marco del SIGRIP, el procedimiento para el reporte de operaciones sospechosas es un mecanismo de protección institucional. Su propósito es garantizar que cualquier situación que sugiera que la entidad está siendo utilizada para dar apariencia de legalidad a recursos de origen ilícito o para canalizar fondos hacia actividades terroristas sea identificada, analizada y puesta en conocimiento de las autoridades competentes de manera oportuna.

En este sentido, se espera que las entidades distritales implementen este componente de manera articulada con todos sus procesos, garantizando su operatividad, trazabilidad y capacidad de respuesta oportuna frente a señales de alerta, en coherencia con los lineamientos definidos en el presente numeral.

**a. Definiciones operativas esenciales[14]**

Para efectos de la presente estrategia, se adoptan las siguientes definiciones:

- ✓ *Una operación inusual:* es aquella cuya cuantía, características, frecuencia, origen, destino o circunstancias se apartan de los patrones normales de la actividad institucional o del perfil conocido de la contraparte, sin que ello implique necesariamente la existencia de un delito. Su identificación activa el proceso interno de análisis.[15]

[14] Para efectos de la presente estrategia, estas definiciones operativas sistematizan conceptos contenidos en documentos técnicos e instructivos de la UIAF y en los demás referentes normativos y técnicos desarrollados en el marco conceptual, sin sustituir ni modificar las definiciones establecidas en las disposiciones que resulten aplicables.

[15] La negativa injustificada de la contraparte a suministrar información solicitada en el marco de la debida diligencia o del análisis de una operación inusual es en sí misma una señal de alerta que puede contribuir a determinar el carácter sospechoso de la operación.

- ✓ *Una operación sospechosa:* es aquella operación inusual respecto de la cual, luego del análisis correspondiente, no es posible encontrar una explicación razonable que justifique su carácter atípico, generando una presunción fundada de que podría estar vinculada con actividades de LA/FT/FP. Su determinación activa la obligación de reporte ante las autoridades competentes.
- ✓ *Una operación intentada:* es aquella que no llegó a iniciarse o completarse porque fue rechazada, suspendida, frustrada o abandonada y cuyas circunstancias activaron una o más señales de alerta. Su identificación da lugar al análisis interno correspondiente. Será objeto de ROS cuando, después del análisis, existan elementos objetivos que permitan calificarla como sospechosa y el reporte resulte aplicable a la entidad.[16]
- ✓ *Reporte de Ausencia de Operaciones Sospechosas (AROS):* es el reporte negativo que debe presentar una entidad reportante cuando, durante el período correspondiente, no se hayan identificado operaciones o situaciones que deban ser reportadas a la UIAF, de acuerdo con las reglas aplicables al sector bajo el cual se encuentre registrada. Su presentación se realizará a través del SIREL, cuando la obligación esté prevista en la normativa, los anexos técnicos, los instructivos o las demás disposiciones expedidas por la UIAF, y con sujeción a las condiciones, términos y periodicidad que esta determine. (Unidad de Información y Análisis Financiero - UIAF, 2020).

La distinción entre operación inusual y sospechosa es fundamental debido a que no toda operación inusual es sospechosa, pero toda operación sospechosa fue primero inusual. El análisis que media entre las dos es la responsabilidad central del responsable de la función de cumplimiento.

**b. Procedimiento orientador para la identificación, análisis y reporte de operaciones inusuales y sospechosas.**

Cada entidad del Distrito Capital documentará y aprobará un procedimiento interno para la identificación, análisis y reporte de operaciones inusuales y sospechosas *(que puede formar parte del Manual de Debida Diligencia o como documento independiente),* por lo que se presenta la ruta completa desde la identificación de una señal de alerta, hasta el reporte ante la autoridad competente. Ruta diseñada para que cualquier entidad distrital pueda adoptarla como base de su procedimiento interno, adaptándola a su contexto y capacidades.

Cada entidad establecerá en su procedimiento interno los términos para la recepción, revisión, análisis, escalamiento y decisión sobre las operaciones reportadas, teniendo en cuenta su estructura, capacidad operativa, nivel de exposición al riesgo y régimen aplicable. Estos términos deberán favorecer la inmediatez del análisis y del reporte externo cuando corresponda, sin afectar la suficiencia, objetividad y trazabilidad de la evaluación realizada.

La ruta tiene cuatro momentos que corresponden a cuatro actores distintos: el servidor o colaborador de la entidad que identifica la señal, el líder de proceso que gestiona el reporte interno, el responsable de la función de cumplimiento que analiza y decide, y la entidad que reporta ante la autoridad externa.

[16] La obligación de reportar las operaciones intentadas está expresamente establecida en la Guía V7 del DAFP (2025), numeral 6.3.5.4, y es coherente con el enfoque preventivo del sistema: el riesgo para la integridad pública existe desde el momento en que se intenta la operación, con independencia de si se consumó.

**MOMENTO 1 Identificación de la señal de alerta**

**Actor principal:** cualquier servidor o colaborador de la entidad

***Paso 1.1 Reconozca si la situación activa una señal de alerta***

Cualquier servidor o colaborador que, en el ejercicio de sus funciones u obligaciones, observe una situación que se aparte del comportamiento esperado de una contraparte debe preguntarse: ¿esto corresponde al patrón normal de esta operación o de esta contraparte?

Las señales de alerta son las situaciones, comportamientos, documentos u operaciones que, por resultar atípicos, requieren un análisis adicional. Para facilitar su identificación, la entidad podrá apoyarse en la C*aja de Herramientas para la Prevención de Riesgos de LA/FT/FPADM, versión 2.0,* elaborada por la Secretaría General de la Alcaldía Mayor de Bogotá con el apoyo de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), disponible en el **Anexo 4,** en particular en el documento *"Escenarios de riesgo de lavado de activos y señales de alerta en las entidades del Distrito Capital"*, que ofrece ejemplos y escenarios aplicables a la gestión pública distrital. Este instrumento es de carácter orientador, por lo que las señales no se consideran taxativas y podrán complementarse conforme a las particularidades de cada entidad.

Adicionalmente, se recomienda que cada entidad identifique y realice seguimiento a aquellos procesos, operaciones, actividades o relaciones con terceros que, de acuerdo con su contexto institucional y análisis de riesgos, representen una mayor exposición a riesgos LA/FT/FP. Lo anterior permitirá detectar oportunamente comportamientos inusuales, inconsistencias o situaciones que puedan constituir señales de alerta y requerir una revisión más detallada. A partir esto las señales de alerta identificadas se documentarán y mantendrán actualizadas, de manera que sirvan de insumo para el monitoreo y la gestión de los riesgos de LA/FT/FP.

Se recomienda, que las entidades fortalezcan sus programas de capacitación, incorporando ejercicios prácticos de identificación de señales de alerta en el contexto específico de sus operaciones o transacciones.

La concurrencia de varias señales puede incrementar el nivel de exposición y justificar un análisis más profundo, sin que ello permita concluir automáticamente que existe una operación sospechosa. Cuando la situación lo amerite, se recomienda involucrar las instancias, dependencias o equipos que cada entidad considere pertinentes, de acuerdo con su estructura organizacional, esquema de gobierno y procedimientos internos, con el fin de apoyar el análisis de la situación y la definición de las acciones que correspondan.

***Paso 1.2 Orientación para quien identifica y reporta la situación:* no investigue por su cuenta**

Cuando un servidor o colaborador de la entidad identifique una situación inusual, su responsabilidad se concentra en reportarla oportunamente. No debe investigar por su cuenta, confrontar a la contraparte sobre sus sospechas ni abstenerse de reportar por temor a equivocarse. Una vez presentado el reporte, mantendrá la reserva, preservará los soportes disponibles y atenderá las solicitudes de información o aclaración que formulen las instancias competentes.

El reporte presentado de buena fe está protegido y no genera, por sí mismo, responsabilidad para quien lo formula, aun cuando, después del análisis, la operación no sea calificada como sospechosa (Ley 190, 1995). La persona que reporte de buena fe no será objeto de consecuencias adversas por la sola presentación del reporte, siempre que este se fundamente en hechos, documentos o circunstancias que razonablemente considere relevantes.

Esta protección no ampara los reportes presentados de mala fe ni el uso indebido del procedimiento, sin perjuicio de las responsabilidades que puedan derivarse conforme al marco jurídico aplicable.

Para que el reporte funcione de manera efectiva, es importante que la entidad formalice esta garantía en su procedimiento interno y establezca mecanismos para prevenir y gestionar represalias, proteger la identidad del reportante cuando resulte procedente y conservar la trazabilidad y la reserva del reporte.

***Paso 1.3 Reporte la situación al líder de proceso***

El servidor o colaborador comunicará la situación al líder de su proceso o directamente al responsable de la función de cumplimiento cuando exista conflicto de interés, posible participación del líder, necesidad especial de reserva, urgencia o cuando así lo defina la entidad, utilizando el canal reservado dispuesto para la gestión de reportes asociados a riesgos de LA/FT/FP. El reporte deberá contener, como mínimo, la descripción objetiva de la situación observada; la fecha y el proceso en que ocurrió; la identificación de la contraparte involucrada; y cualquier documentación de soporte disponible.

**MOMENTO 2 Reporte interno al responsable de la función de cumplimiento.**

**Actor principal:** líder de proceso

***Paso 2.1 Reciba y valore el reporte del servidor o colaborador de la entidad.***

El líder de proceso recibe el reporte del servidor o colaborador de la entidad y realiza una primera valoración para determinar si la situación efectivamente corresponde a una señal de alerta. Esta valoración no implica investigación: consiste en verificar si lo reportado coincide con las señales de alerta identificadas y documentadas por la entidad.

***Paso 2.2 Recopile la información disponible***

Antes de escalar el caso al responsable de la función de cumplimiento, el líder de proceso reunirá toda la información disponible sobre la operación y la contraparte: documentos del proceso, antecedentes de la relación, registros de comunicaciones, resultados previos de debida diligencia, entre otros. Esta información es el insumo del análisis que realizará el responsable de la función de cumplimiento.

***Paso 2.3 Escale el caso al responsable de la función de cumplimiento***

Una vez verificada la activación de una señal de alerta, el líder de proceso deberá escalar el caso al responsable de la función de cumplimiento, quien será el encargado de coordinar el análisis

posterior y determinar la ruta institucional correspondiente utilizando el formato de Reporte de Operación Inusual (ROI).[17]

La entidad definirá, al adoptar y/o adaptar este procedimiento, el plazo máximo para remitir el ROI, teniendo en cuenta la urgencia, el nivel de riesgo y las características de sus operaciones. En todo caso, el reporte deberá realizarse oportunamente y sin demoras injustificadas que puedan afectar la conservación de la información, permitir la continuación de la operación o comprometer la oportunidad del análisis. Cuando se presente alguna de estas circunstancias, el caso se escalará de manera inmediata, con la información y los soportes disponibles, sin perjuicio de que posteriormente se complemente el reporte.

**MOMENTO 3 Análisis y determinación del carácter sospechoso.**

**Actor principal:** responsable de la función de cumplimiento

***Paso 3.1 Acuse recibo y abra el caso***

Una vez recibido el ROI, el responsable de la función de cumplimiento acusará recibo, registrará el caso y dará inicio a su análisis, garantizando la trazabilidad de las actuaciones realizadas.

Los tiempos para analizar el ROI y adoptar una decisión corresponden a criterios internos que cada entidad deberá definir al adoptar y/o adaptar este procedimiento, teniendo en cuenta la urgencia, complejidad, nivel de riesgo, disponibilidad de información y características de sus operaciones. Estos tiempos deberán establecer un plazo máximo para la gestión del caso y evitar demoras injustificadas que puedan afectar la oportunidad del análisis o del eventual reporte externo.

Cuando la situación pueda comprometer la conservación de la información, permitir la continuación de la operación o incrementar la exposición de la entidad, el análisis se adelantará de manera prioritaria.

Los tiempos internos previstos para gestionar el ROI no modifican la obligación de remitir el ROS de manera inmediata a la UIAF, una vez la entidad determine que la operación es sospechosa, de acuerdo con las instrucciones emitidas por dicha Unidad.

Se entenderá por inmediato el momento a partir del cual la entidad identifica una operación como sospechosa, ya sea realizada o intentada. Para estos efectos, no se requiere que la entidad tenga certeza sobre la existencia de una actividad delictiva, identifique un tipo penal específico o verifique el origen ilícito de los recursos. Basta con que la operación presente características de sospecha conforme a los criterios definidos por la UIAF y los instrumentos internos adoptados por la entidad. [18]

***Paso 3.2 Realice el análisis de la operación inusual***

[17] La Caja de Herramientas para la Prevención de Riesgos de LA/FT/FPADM, versión 2.0, elaborada por la Secretaría General de la Alcaldía Mayor de Bogotá con el apoyo de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), disponible en el Anexo 4., contiene el segmento denominado FORMATOS que contiene los formatos de Reporte de Operaciones Inusuales (ROI) y el formato de Operaciones Sospechosas (ROS) que sirven como guía para que la Entidad pueda implementarlos.

[18] Definición adaptada del Anexo 1. Documento técnico e instructivo para el reporte de operaciones sospechosas de las entidades obligadas a reportar bajo la Ley 2195 de 2022 de la UIAF.

El responsable de la función de cumplimiento analiza la operación inusual con el objetivo de determinar si existe una explicación razonable que justifique su carácter atípico, o si por el contrario existen elementos objetivos que permitan considerar que podría estar vinculada con actividades de LA/FT/FP.

El análisis incluirá, según las características del caso, las siguientes verificaciones:

- ✓ *Contraste con el perfil de la contraparte*: revise la información obtenida y actualizada mediante la debida diligencia para determinar si la situación identificada es consistente con la actividad, el tamaño, las operaciones y el historial conocido de la contraparte. También valore si existen cambios relevantes en su estructura, representación, beneficiarios finales, actividad u otra información que puedan explicar la situación.
  Esta revisión no implica repetir integralmente la debida diligencia. Cuando la información disponible sea insuficiente, presente inconsistencias o requiera actualización, el responsable de la función de cumplimiento podrá solicitar su ampliación o verificación a través de la dependencia o el equipo que gestiona directamente la operación o la relación con la contraparte, preservando la reserva del análisis.
- ✓ *Verificación en fuentes de información*: efectúe la consulta actualizada en listas vinculantes y restrictivas y revise la información pública disponible. Según el tipo de relación y el régimen aplicable, podrán consultarse fuentes oficiales como el Boletín de Responsables Fiscales de la Contraloría General de la República, el Sistema de Información para el Registro de Sanciones y Causas de Inhabilidad (SIRI) de la Procuraduría General de la Nación, los antecedentes judiciales administrados por la Policía Nacional, el Registro Nacional de Medidas Correctivas, el Registro Único Empresarial y Social (RUES) y otras fuentes pertinentes.
  La consulta al Registro Único de Beneficiarios Finales (RUB) se realizará únicamente cuando la entidad se encuentre legalmente habilitada para acceder a su información. Los resultados de las consultas se analizarán de acuerdo con la naturaleza de la fuente y no generarán automáticamente la calificación de la operación como sospechosa.
- ✓ *Análisis de la operación en su contexto*: determine si la operación es coherente con el objeto del contrato o de la relación institucional, y si sus montos, frecuencia, condiciones, participantes y demás características son consistentes con la información conocida de la contraparte, valorándose si la operación cuenta con una justificación técnica, económica o institucional razonable.
- ✓ *Solicitud de información adicional a la contraparte*: cuando resulte pertinente, el responsable de la función de cumplimiento podrá solicitar, a través la dependencia o el equipo que gestiona directamente la operación o la relación con la contraparte, información o documentación adicional que permita verificar la situación. La solicitud se formulará como un requerimiento ordinario de conocimiento, verificación o actualización de información, sin revelar la existencia de señales de alerta, análisis internos, evaluación de sospecha o un eventual reporte.
  La falta de respuesta o la negativa injustificada para suministrarla podrá considerarse una señal de alerta adicional, de acuerdo con las circunstancias del caso.
- ✓ *Reserva y manejo de la información del análisis:* la documentación asociada al análisis se manejará con acceso restringido, trazabilidad, seguridad de la información y protección de datos personales, y se conservará de conformidad con las tablas de retención documental y los instrumentos archivísticos aplicables en la entidad.

No se revelará a la contraparte ni a terceros no autorizados la existencia del análisis, la evaluación del carácter sospechoso de la operación o la eventual elaboración de un reporte.

El análisis documentará los hechos verificados, las fuentes consultadas, la información valorada, las explicaciones obtenidas, las limitaciones encontradas y los elementos que servirán de fundamento para adoptar la decisión prevista en el siguiente paso.

***Paso 3.3 Documente el análisis y adopte una decisión motivada***

El responsable de la función de cumplimiento documentará el análisis realizado, incluidos los hechos verificados, las fuentes consultadas, la información y los soportes valorados, las explicaciones obtenidas, las señales de alerta identificadas y las limitaciones encontradas. Con fundamento en estos elementos, adoptará una decisión motivada.

La documentación del análisis permitirá verificar que la decisión fue objetiva, razonable y trazable, sin que ello implique que la entidad deba acreditar la existencia de un delito o establecer responsabilidades.

Como resultado del análisis, podrán adoptarse las siguientes decisiones:

***La operación tiene una explicación razonable***: se documentará la conclusión, se cerrará el caso y se adoptarán las medidas de monitoreo que correspondan. No se presentará ROS ante la UIAF.

***La operación es sospechosa***: se determina que no existe una explicación razonable que justifique su carácter atípico y que existen elementos objetivos para calificarla como sospechosa. En este caso, la entidad actuará de acuerdo con su calidad de reportante, las instrucciones de la UIAF y el procedimiento previsto en el Momento 4.

***Se requiere información adicional***: se solicitará la información necesaria antes de adoptar la decisión final. La función de cumplimiento establecerá en el requerimiento un término concreto y razonable para su atención, considerando la complejidad, urgencia y nivel de riesgo del caso.

Cada entidad definirá, al adoptar y/o adaptar este procedimiento, el plazo máximo para analizar el ROI y adoptar una decisión. Este plazo deberá evitar demoras injustificadas y podrá contemplar un tratamiento prioritario para los casos cuya demora pueda afectar la conservación de la información, permitir la continuación de la operación o incrementar la exposición de la entidad.

Cuando se determine que la operación es sospechosa, los tiempos internos de análisis no modificarán la obligación de enviar el ROS de manera inmediata a la UIAF, conforme a las instrucciones aplicables.

En todos los casos, la decisión deberá quedar consignada en el expediente reservado, con la fecha, la identificación del responsable de la función de cumplimiento, los fundamentos de la conclusión y los soportes correspondientes.

***Paso 3.4 Tratamiento especial: operaciones intentadas***[19]

Cuando la situación inusual corresponda a una operación intentada, es decir, aquella que no llegó a consumarse porque fue rechazada por la entidad, porque la contraparte desistió al ser requerida o porque fue frustrada por cualquier causa, el procedimiento de análisis será el mismo que se aplica a una operación consumada.

Si, como resultado de dicho análisis, se identifican elementos objetivos que permitan calificar la operación como sospechosa, se aplicará la ruta de reporte prevista para la entidad, precisando que la operación no se consumó. En estos casos existe la misma obligación de reportar ante la UIAF que para una operación efectivamente realizada.

Por el contrario, cuando el análisis permita establecer una explicación razonable, se documentará la conclusión y se adoptarán las medidas de monitoreo que correspondan, sin que ello dé lugar a reporte.

Las entidades distritales deben interiorizar que la obligación de reporte no depende de si la operación se consumó o no, sino de si, después del análisis, existen elementos objetivos que permitan concluir que la operación estaría vinculada con actividades de LA/FT/FP.

**MOMENTO 4 Reporte ante las autoridades competentes.**

**Actor principal:** responsable de la función de cumplimiento

***Paso 4.1 Elabore el Reporte de Operación Sospechosa (ROS)***

Una vez determinado el carácter sospechoso de la operación, el responsable de la función de cumplimiento elabora el Reporte de Operación Sospechosa (ROS) siguiendo el formato y los parámetros establecidos por la UIAF[20], los que adicionalmente se encuentran incorporados en el Formato de Operaciones Sospechosas del (Anexo 4) denominado *Caja de Herramientas para la prevención riesgos de LA/FT/FPADM V2.0,* que podrá ser adoptado por la entidad.

*La descripción de la operación sospechosa:*

La descripción de la operación es el elemento más determinante del ROS, pues es la que permite a la UIAF realizar inteligencia financiera efectiva. Debe ser clara, completa y ordenada, sin omitir datos conocidos, aunque sean detalles que parezcan menores.

*Ilustración 5 Importancia de los ROS en los Sistemas Anti LA/FT/FP*

[19] La Guía V7 del DAFP (2025) establece expresamente que el procedimiento debe contemplar el reporte de operaciones sospechosas "incluso cuando fue intentada". Esta disposición es coherente con el enfoque de la gestión del riesgo de LA/FT/FP, que busca prevenir la utilización de la entidad como instrumento, independientemente de si la operación llegó a consumarse.

[20] El formato del ROS y el instructivo para su elaboración están disponibles en www.uiaf.gov.co, sección reportantes, en el sector correspondiente a cada entidad.




Fuente: Elaboración propia con base en Guía de buenas prácticas del ROS (UIAF, 2020).

La imagen presenta de manera gráfica la importancia del Reporte de Operaciones Sospechosas (ROS) dentro del sistema de prevención del LA/FT/FP. En ella se evidencia cómo los ROS cumplen un rol estratégico al prevenir y detectar delitos

*¿Que debe incluir un ROS?*

- Copias de los documentos que respaldan la descripción de la operación sospechosa
- Informaciones detalladas sobre las partes involucradas
- Información sobre los productos y servicios relacionados con la operación
- Una descripción objetiva del contexto económico de la operación y, cuando aplique, la condición de Persona Expuesta Políticamente (PEP) de las personas involucradas.
- Una descripción de las señales de alerta o comportamientos inusuales.
- Detalles específicos en la relatoría de las sospechas encontradas.

En lo que corresponde a la estructura de un Reporte de Operación Sospechosa (ROS), es útil organizar la información siguiendo las preguntas clave que aparecen en la siguiente quién, qué, cuándo, dónde y por qué.

*Ilustración 6 Estructura de un ROS*




Fuente: Elaboración propia con base en *Guía de buenas prácticas del ROS* (UIAF, 2020).

En primer lugar, se debe identificar claramente quiénes son las contrapartes involucradas en la operación reportada, ya sean clientes, terceros o beneficiarios finales. Luego, se describe qué operación se realizó o intentó realizar, especificando su naturaleza, características y cualquier comportamiento inusual asociado. También es fundamental precisar cuándo ocurrieron los hechos, incluyendo fechas exactas o rangos de tiempo relevantes.

Asimismo, se debe indicar dónde tuvieron lugar las transacciones o actividades, detallando locaciones físicas, canales o medios utilizados. Finalmente, se expone por qué la operación genera sospecha, es decir, la señal de alerta o el patrón detectado que motiva el reporte. Esta estructura permite presentar un ROS claro, completo y coherente, facilitando el análisis por parte de la UIAF.

**Nota:** La Secretaría General invita a las entidades distritales a consultar y aplicar el (Anexo 4) denominado *Caja de Herramientas para la prevención riesgos de LA/FT/FPADM V2.0*, la cual integra instrumentos metodológicos para su implementación. En particular, la "*Hoja de ruta para la implementación de la caja de herramientas de gestión de riesgos LA/FT/FPADM"* Estos insumos podrán ser utilizados como referentes técnicos para orientar la implementación progresiva del componente en las entidades, de acuerdo con su contexto institucional.

Allí se encontrarán cuatro módulos específicos sobre debida diligencia: Módulo de Debida diligencia, Modulo Formatos ROI-ROS, Módulo de Listas de Consultas, Módulo de Segmentación.

***Paso 4.2 Envíe el ROS a través del SIREL***

Cuando la entidad tenga la calidad de reportante o se encuentre habilitada ante la UIAF, el ROS será enviado mediante el Sistema de Reporte en Línea (SIREL), de acuerdo con el sector, formato e instrucciones. [21]

Es importante que la entidad verifique y mantenga documentado aspectos como: su calidad de reportante, el sector o categoría bajo la cual se encuentra registrada, la vigencia de los usuarios y credenciales, los responsables autorizados para operar SIREL.

Cuando la entidad no tenga calidad de reportante o no se encuentre habilitada, deberá consultar y aplicar las orientaciones vigentes de la UIAF para su situación particular. La información asociada al caso no deberá remitirse mediante correos, formularios o canales no autorizados que comprometan su reserva. El ROS está amparado por reserva legal, por lo que su existencia, contenido y tratamiento deben mantenerse bajo estricta confidencialidad entre la entidad reportante y la UIAF (Ley 526, art.9 , 1999)

La falta de habilitación en el SIREL no exime a la entidad de documentar y analizar la situación, gestionar sus riesgos y evaluar las demás acciones contractuales, administrativas, disciplinarias, fiscales o penales que resulten procedentes.

***Paso 4.3. Presente el Reporte de Ausencia de Operaciones Sospechosas (AROS), cuando resulte aplicable***

Cuando resulte aplicable, de acuerdo con el ámbito definido en el numeral 2.5.1 y las instrucciones vigentes de la UIAF para el sector correspondiente, la entidad presentará a través

[21]Para información sobre el registro, habilitación y administración de usuarios en el SIREL, consulte las instrucciones vigentes publicadas por la UIAF en: https://www.uiaf.gov.co/node/1344

del Sistema de Reporte en Línea (SIREL) el Reporte de Ausencia de Operaciones Sospechosas (AROS).

El AROS es el reporte negativo mediante el cual la entidad informa que, durante el período correspondiente, no identificó operaciones o situaciones que debieran ser reportadas a la UIAF. Su presentación se realizará con la periodicidad, dentro de los plazos y conforme a las condiciones técnicas establecidas en la normativa, los anexos técnicos o los instructivos vigentes de la UIAF. (Unidad de Análisis Financiero - UIAF, 2025)

La entidad conservará la evidencia de la presentación del AROS y verificará periódicamente las condiciones aplicables a esta obligación.

***Paso 4.4 Evalúe si proceden otras actuaciones***

La presentación del ROS ante la UIAF no sustituye la evaluación de otras actuaciones que puedan resultar procedentes. En consecuencia, cuando los hechos identificados puedan activar un deber de denuncia o de traslado, el responsable de la función de cumplimiento, con el apoyo de la oficina jurídica o de la dependencia competente, evaluará si adicionalmente proceden, entre otras, las siguientes actuaciones:

- Una denuncia ante la fiscalía general de la Nación u otra autoridad competente.
- Un traslado disciplinario o fiscal.
- Una actuación contractual o administrativa.
- La activación del canal institucional de denuncias.
- Otras medidas preventivas o correctivas.

Estas actuaciones son independientes del ROS y se tramitará por los canales correspondientes, sin anexar ni revelar su contenido reservado, salvo que exista fundamento jurídico para ello.

La evaluación institucional no constituye una declaración sobre la existencia de un delito o de una responsabilidad, competencia que corresponde a las autoridades respectivas.[22]

***Paso 4.5 Documente, cierre y custodie el expediente del caso***

Una vez adoptada la decisión final, el responsable de la función de cumplimiento documentará el cierre del caso y conformará el expediente reservado con el Reporte de Operación Inusual (ROI), sus soportes, el análisis realizado, las fuentes consultadas, las conclusiones y la decisión motivada. Cuando se haya presentado un Reporte de Operación Sospechosa (ROS), se incluirán también el reporte elaborado, el comprobante de envío a través del SIREL y las comunicaciones relacionadas con el caso.

La custodia funcional del expediente y la administración de sus accesos corresponderán a la función de cumplimiento o a la persona o dependencia formalmente designada por la entidad. El acceso se limitará a las personas autorizadas y a las autoridades que cuenten con competencia y fundamento jurídico para solicitar la información.

El expediente deberá conservarse durante el término establecido en la normativa aplicable y en la Tabla de Retención Documental de la entidad, respetando los periodos mínimos obligatorios.

[22] El ROS ante la UIAF y la denuncia ante la fiscalía general de la Nación son actuaciones independientes y complementarias, que atienden finalidades distintas.

Para las entidades a las que resulte aplicable el instructivo de la UIAF para los sujetos obligados bajo la Ley 2195 de 2022, los soportes de la operación reportada se conservarán como mínimo durante cinco años, sin perjuicio de términos especiales. (Unidad de Análisis Financiero - UIAF, 2025)

El expediente reservado se mantendrá separado de otros expedientes *(contractuales, administrativos, disciplinarios, laborales o de auditoría ordinaria, entre otros*). Cuando resulte necesario adelantar otras actuaciones institucionales, se utilizará únicamente la información pertinente, sin anexar ni revelar el ROS o su contenido, salvo que exista fundamento jurídico para ello.

***Paso 4.6 Retroalimente el SIGRIP***

Cada caso gestionado, independientemente de si dio lugar o no a un ROS, retroalimentará el SIGRIP.

La determinación de una operación como sospechosa y la presentación del ROS no constituyen, por sí mismas, la materialización del riesgo ni la comprobación de una conducta ilícita. El ROS es un mecanismo reservado de reporte que pone la información en conocimiento de la UIAF para el ejercicio de sus funciones, mientras que la calificación de una conducta como delito corresponde a las autoridades competentes.

En consecuencia, la materialización del riesgo no se deriva de la presentación de un ROS, sino del análisis de si los hechos gestionados corresponden al evento de riesgo LA/FT/FP formulado en el mapa institucional. Con fundamento en dicho análisis, el responsable de la función de cumplimiento evaluará si el caso justifica adoptar acciones de mejora o fortalecimiento del SIGRIP, entre las cuales podrán considerarse, según corresponda:

a) Actualizar las señales de alerta documentadas por la entidad.
b) Ajustar o fortalecer los controles asociados en el mapa de riesgos.
c) Revisar la valoración del riesgo, ajustando su probabilidad o impacto con base en la evidencia del caso.
d) Reforzar la debida diligencia para determinado tipo de contrapartes u operaciones.
e) Incluir el caso, de manera anonimizada, en los programas de capacitación.
f) Otras acciones que la entidad considere pertinentes para fortalecer la prevención y gestión del riesgo.

Todas estas acciones se adelantarán respetando la reserva de la información y utilizando datos anonimizados que no permitan identificar a las personas involucradas ni revelar el contenido del ROS.

# Capítulo 3 Función de Cumplimiento

## 3.1. Contexto Normativo y alcance transversal

La función de cumplimiento constituye un mecanismo institucional orientado a promover el adecuado funcionamiento del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), mediante la coordinación, seguimiento, evaluación y mejora continua de sus procesos. Se concibe como un elemento transversal del sistema, aplicable a la gestión de las amenazas

para la integridad pública *corrupción, fraude interno, soborno, inadecuada gestión de conflictos de interés y LA/FT/FP.* En consecuencia, sus principios, responsabilidades y condiciones de ejercicio operan de manera común frente a los distintos componentes del SIGRIP, sin perjuicio de las responsabilidades específicas que en materia de LA/FT/FP le corresponden conforme a la presente estrategia.

En el Distrito Capital, los antecedentes de este componente pueden identificarse en la (Circular 092 , 2020), mediante la cual se promovió la implementación del Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo (SARLAFT) en las entidades distritales, así como en la Ruta Metodológica para la Implementación del SARLAFT, el Lineamiento para Implementar el Sistema de Administración de Riesgos del Lavado de Activos y Financiación del Terrorismo en las Entidades del Distrito (Ruta Metodológica SARLAFT, 2021), y el Documento Técnico Adaptación de medidas de prevención y mitigación del riesgo del lavado de activos y financiación del terrorismo en las entidades del Distrito Capital (Documento Técnico de Adaptación Medidas de Prevención y Mitigacion - SARLAFT, 2022). Estos instrumentos desarrollaron conceptos, metodologías, responsabilidades institucionales y mecanismos de coordinación orientados a fortalecer la gestión preventiva de los riesgos LA/FT/FP.

La consolidación de la función de cumplimiento como componente institucional se produce con la expedición de la Ley 2195 de 2022 y su posterior desarrollo a través de la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7, la cual incorpora la función de cumplimiento como elemento estructural del SIGRIP y define sus responsabilidades en materia de monitoreo, evaluación, articulación institucional, mejora continua, adopción de lineamientos y gestión de reportes asociados a los riesgos para la integridad pública.

En el ámbito distrital, el alcance transversal de la función de cumplimiento se articula con la Política de Cumplimiento Normativo, componente del Modelo de Gestión Jurídica Anticorrupción (MGJA). El modelo se integra por seis componentes: la política de cumplimiento normativo, el órgano de cumplimiento, el plan de cumplimiento normativo, las líneas de aseguramiento, las políticas de alerta de irregularidades y los incentivos a la innovación y buenas prácticas en materia de integridad y ética de lo público[23]. Dado que la política de cumplimiento normativo comprende el compromiso de cumplir todas las normas jurídicas de integridad, transparencia y lucha contra la corrupción administrativa, la función de cumplimiento del SIGRIP se entiende articulada con el Órgano de Cumplimiento previsto en el MGJA, evitando duplicidades y favoreciendo la coordinación institucional. Esta articulación no implica que el SIGRIP asuma una función general de cumplimiento normativo, sino que, dentro de su ámbito, contribuye al cumplimiento de las obligaciones aplicables relacionadas con la gestión de los riesgos para la integridad pública.

En consecuencia, la función de cumplimiento no constituye una instancia de control independiente ni sustituye las responsabilidades de las oficinas de control interno o las que hagan sus veces. Por el contrario, actúa como un mecanismo de coordinación, articulación y acompañamiento institucional dirigido a apoyar a la Alta Dirección o a la que haga sus veces al

[23] El MGJA fue adoptado mediante el Decreto Distrital 610 de 2022 compilado en el Título 5 del Decreto Distrital 479 de 2024, Único Distrital del Sector Gestión Jurídica. Conforme al artículo 322 de este último, el modelo se integra por seis componentes.

interior de la entidad en la gestión preventiva de los riesgos para la integridad pública, contribuyendo al fortalecimiento y la efectividad del SIGRIP.

## 3.2. ¿Qué es la función de cumplimiento y por qué es relevante para las entidades distritales?

La función de cumplimiento es el eje articulador del SIGRIP al interior de cada entidad. No se trata de una función meramente formal o documental; es una función estratégica que garantiza que el SIGRIP opere de manera efectiva, que los riesgos se gestionen oportunamente y que la entidad cumpla con sus obligaciones legales en materia de integridad, transparencia y prevención de riesgos para la integridad pública.

En el contexto distrital, la relevancia de esta función es especialmente significativa dado el volumen, la diversidad y la complejidad de las relaciones institucionales que las entidades del Distrito Capital gestionan: contratos, convenios, subsidios, licencias, permisos y vinculaciones con un universo amplio de contrapartes. Esta complejidad exige que exista dentro de cada entidad una persona o grupo de personas con la autoridad, la capacidad técnica y la autonomía necesarias para velar por que los riesgos para la integridad pública sean identificados, analizados y tratados de manera oportuna y proporcional.

La asignación de la función de cumplimiento se desarrollará de manera articulada con la estructura organizacional, las capacidades institucionales y el nivel de madurez de cada entidad distrital. No obstante, lo anterior no implica la flexibilización de las condiciones mínimas de independencia y jerarquía requeridas para garantizar la efectividad de la función, sino el reconocimiento de que su implementación es progresiva y debe adecuarse a las particularidades y contexto institucional de cada entidad.

En coherencia con su carácter transversal, la función de cumplimiento se articulará con el Órgano de Cumplimiento del MGJA conformado en el marco del Comité Institucional de Gestión y Desempeño o del Comité Directivo, según corresponda (artículo 325, Decreto Único Distrital 479 de 2024), así como con las demás instancias responsables de la gestión de riesgos para la integridad en la entidad. Esta articulación respetará el esquema de las tres líneas de aseguramiento, sin absorber ni sustituir las funciones de evaluación independiente propias de la Oficina de Control Interno.

## 3.3. ¿Qué se espera del componente en el SIGRIP Distrital?

En el marco del SIGRIP, la función de cumplimiento actúa como segunda línea de aseguramiento, lidera la coordinación técnica de la implementación del componente de gestión de riesgos LA/FT/FP y proporciona orientación técnica, acompañamiento, monitoreo y consolidación de información para apoyar la gestión de los riesgos para la integridad pública. Su ejercicio no sustituye las responsabilidades de la Alta Dirección y de los comités institucionales competentes en el direccionamiento estratégico; de los líderes de proceso, servidores y colaboradores en la ejecución de los controles y el monitoreo de primera línea; ni de la Oficina de Control Interno o quien haga sus veces en la evaluación independiente de tercera línea. En todo caso, cada proceso conserva la responsabilidad sobre la gestión de sus riesgos.

Las responsabilidades de la función de cumplimiento comprenden:

i. Velar, desde su rol de segunda línea de aseguramiento, por el funcionamiento integral del SIGRIP, asegurando que todos sus componentes operen de manera efectiva, eficiente, oportuna y articulada, y que los líderes de proceso y gestores de riesgo cuenten con el apoyo técnico necesario para gestionar los riesgos identificados, pudiendo generar para ello políticas y procedimientos internos de carácter vinculante para la entidad.
ii. Evaluar, desde su rol de segunda línea de aseguramiento, periódicamente el SIGRIP y presentar sus resultados a la Alta Dirección o la que haga sus veces, incluyendo el análisis de los reportes de operaciones generados, el estado de los planes de mejoramiento, el resultado de la gestión desarrollada en el marco de la función de cumplimiento y las recomendaciones para fortalecer el sistema.
iii. Revisar y articular la implementación de los lineamientos externos emitidos por el DAFP, la Secretaría de Transparencia de la Presidencia de la República, la UIAF y los organismos de control; promover y adoptar los correctivos que se encuentren dentro de su competencia; y proponer a la Alta Dirección o la que haga sus veces la actualización de los elementos del sistema, velando por su comunicación oportuna a todas las partes interesadas.
iv. Colaborar en el diseño de las metodologías, modelos e indicadores cualitativos y/o cuantitativos que requiera el SIGRIP y aplicarlos según corresponda; establecer los lineamientos institucionales de debida diligencia, promoviendo su aplicación proporcional y basada en riesgos en el conocimiento de las contrapartes; y definir los criterios objetivos para la identificación de operaciones inusuales y sospechosas, los cuales serán sometidos a aprobación de la Alta Dirección o la que haga sus veces.
v. Gestionar los reportes de operaciones sospechosas, canalizando internamente los reportes de los líderes de proceso, analizando su carácter inusual o sospechoso y realizando el reporte externo de las operaciones sospechosas ante la UIAF, de acuerdo con la calidad de reportante o habilitación de la entidad y con el procedimiento institucional adoptado. Cuando del análisis surjan hechos que puedan justificar otras actuaciones, la función de cumplimiento los pondrá en conocimiento de la dependencia institucional competente para que evalúe la ruta aplicable, de acuerdo con la naturaleza de los hechos, las competencias legalmente asignadas y el régimen correspondiente.
vi. Articular con las dependencias correspondientes las gestiones pertinentes para la operatividad del SIGRIP y el desarrollo de los programas internos de capacitación en materia de cumplimiento y gestión del riesgo, promoviendo la cultura de integridad institucional junto con las áreas competentes.
vii. En caso de presentarse, declarar oportunamente cualquier situación que pueda dar lugar a conflictos de interés reales, potenciales o aparentes. Así mismo, actuar conforme a los procedimientos institucionales definidos para su gestión y resolución, garantizando que el ejercicio de la función de cumplimiento se desarrolle con independencia, objetividad y probidad.

**Nota:** Para efectos de la presente estrategia se utiliza la expresión *"función de cumplimiento",* en coherencia con la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7. En las entidades sujetas a un régimen sectorial que exija la designación de un oficial de cumplimiento, dicha figura desarrollará las responsabilidades aquí descritas conforme a las disposiciones que le resulten aplicables.

## 3.4. Asignación y condiciones del ejercicio de la función.

No es necesario crear un cargo específico para ejercer la función de cumplimiento. Esta podrá asignarse a una persona, grupo o dependencia dentro de la planta y estructura existentes de la entidad, teniendo en cuenta su naturaleza jurídica, estructura organizacional, planta de personal, cargas de trabajo, complejidad de las operaciones y nivel de exposición a los riesgos para la integridad pública. En el marco de los artículos 2.2.2.2.1 y 2.2.2.2.2 del Decreto 1083 de 2015, la función podrá ser asumida por servidores del nivel directivo o asesor, cuyas funciones generales sean compatibles con las responsabilidades de cumplimiento.

Para las entidades del Distrito Capital, la asignación atenderá a las siguientes condiciones:

**Nivel jerárquico:** La función de cumplimiento deberá asignarse en el segundo nivel jerárquico de la entidad o en una posición organizacional equivalente que, de acuerdo con su naturaleza jurídica y estructura administrativa, garantice independencia funcional, autoridad suficiente, acceso oportuno a la información y reporte directo a la Alta Dirección o al máximo órgano de dirección o gobierno, según corresponda. Cuando la función sea asignada a una persona, grupo o dependencia del nivel directivo o asesor, deberán preservarse estas condiciones y evitarse su dependencia funcional respecto de los procesos cuyas actividades, controles o gestión de riesgos deba monitorear o evaluar.

***Dedicación:*** Se recomienda que quien ejerza la función de cumplimiento cuente en lo posible con una dedicación exclusiva para el desarrollo de sus responsabilidades. No obstante, cada entidad podrá definir el esquema más adecuado de acuerdo con su tamaño, complejidad, nivel de exposición al riesgo y capacidades institucionales, adoptando las medidas necesarias para preservar la independencia y objetividad en el ejercicio de la función.

***Perfil de probidad:*** Quien ejerza la función de cumplimiento, o haga parte del equipo responsable de su desarrollo, deberá ser una persona reconocida dentro de la entidad por su integridad, comportamiento ético, responsabilidad y compromiso con el cumplimiento de sus deberes. Asimismo, deberá mantener una conducta acorde con los principios de transparencia, legalidad y probidad que orientan la función pública, contar con un desempeño satisfactorio en el ejercicio de sus responsabilidades y dar cumplimiento oportuno a las obligaciones relacionadas con la declaración de bienes y rentas, conflictos de interés y demás deberes aplicables conforme a la normatividad vigente.

***Perfil experiencia laboral y formación profesional***: Para la asignación de la función de cumplimiento, la Alta Dirección tendrá en cuenta las competencias requeridas para su adecuado ejercicio, considerando la educación, formación, experiencia y conocimiento necesarios en gestión de riesgos, integridad pública, cumplimiento, debida diligencia, prevención del LA/FT/FP, análisis de información y funcionamiento institucional. Las condiciones específicas serán definidas por cada entidad de acuerdo con su naturaleza jurídica, estructura, operaciones, nivel de exposición al riesgo y capacidades institucionales.

***Capacitación permanente:*** La entidad debe garantizar la formación continua de quien ejerce la función en gestión de riesgos, transparencia, integridad, sistemas antisoborno, antifraude y lineamientos sobre LA/FT/FP.

**Apoyo técnico especializado:** De manera excepcional, cuando la entidad acredite que no cuenta con personal suficiente en su planta para apoyar adecuadamente el ejercicio de la función de cumplimiento, podrá contratar servicios profesionales especializados, de conformidad con la normativa contractual vigente y con las condiciones previstas en la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7. (DAFP, 2025, numeral 6.3.5.3).

Dicho apoyo podrá orientarse al fortalecimiento metodológico, técnico, operativo o de capacitación asociado a la implementación del SIGRIP y a la gestión de los riesgos para la integridad pública.

La contratación de servicios profesionales especializados constituye un mecanismo de apoyo y no implica la transferencia ni la tercerización integral de la función de cumplimiento. En consecuencia, la entidad deberá definir la persona, grupo o dependencia encargada de orientar y supervisar el apoyo contratado, articular sus resultados y asegurar su incorporación en la gestión institucional, sin perjuicio de las responsabilidades de la Alta Dirección o la que haga sus veces, los líderes de proceso, la Oficina de Control Interno y las demás instancias que intervienen en el SIGRIP.

La selección del apoyo garantizará que la persona natural o jurídica contratada cuente con la formación específica y la experiencia relacionada exigidas por la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, en materias asociadas con cumplimiento, gestión de riesgos en entidades públicas, gestión del riesgo LA/FT/FP o asuntos afines con el SIGRIP. Asimismo, deberán observarse las demás condiciones previstas en dicha Guía para la contratación excepcional de particulares que apoyen la gestión de cumplimiento.

**Nota:** La función de cumplimiento no sustituye, elimina ni restringe las funciones propias de las unidades u oficinas de control interno. Ambas instancias son complementarias y su articulación efectiva es una condición para el funcionamiento integral del SIGRIP. La función de cumplimiento se enfoca en la gestión preventiva de los riesgos de integridad pública; el control interno verifica el cumplimiento de los controles y la eficacia del sistema en su conjunto.

# Capítulo 4 Debida diligencia en el conocimiento de las contrapartes

## 4.1. Contexto y alcance del componente.

Las entidades públicas establecen permanentemente relaciones con terceros para el desarrollo de sus funciones, la ejecución de recursos, la prestación de servicios, la implementación de programas y el cumplimiento de sus objetivos misionales. En este contexto, la capacidad de una entidad para conocer razonablemente con quién se relaciona y en qué condiciones lo hace constituye una condición básica de la gestión íntegra de los recursos públicos.

La debida diligencia constituye un mecanismo preventivo orientado a fortalecer la integridad pública mediante el conocimiento, análisis y monitoreo de las relaciones institucionales con terceros, con el fin de identificar, mitigar y gestionar los riesgos asociados a dichas relaciones. Su aplicación no es exclusiva del sector financiero: cualquier entidad que administre recursos públicos, suscriba contratos, otorgue subsidios, ejecute convenios o habilite a terceros para actuar en su nombre está expuesta a riesgos que pueden prevenirse a través de este mecanismo.

El principio de debida diligencia fue incorporado expresamente en el artículo 12 de la Ley 2195 de 2022, que establece la obligación de las entidades del Estado de implementar medidas orientadas a identificar las contrapartes con las que suscriben contratos o convenios, y a conocer el origen de sus recursos. Esta disposición se articula con lo previsto en el artículo 27 de la Ley 1121 de 2006, que impone a las entidades estatales y territoriales la obligación de identificar plenamente a las personas naturales y jurídicas que suscriban contratos, así como el origen de sus recursos, como medida de prevención del uso indebido de los recursos públicos, el lavado de activos y la financiación del terrorismo.

Asimismo, el artículo 31 de la Ley 2195 de 2022, que modificó el artículo 73 de la Ley 1474 de 2011 (Estatuto Anticorrupción), fortaleció los Programas de Transparencia y Ética Pública (PTEP) como instrumentos de prevención frente a la corrupción, incorporando la debida diligencia como uno de sus componentes esenciales en el marco del SIGRIP.

En articulación con lo anterior, la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 7 del DAFP (2025) reconoce la debida diligencia como uno de los componentes de la gestión integral del riesgo de integridad y establece orientaciones específicas para su incorporación en los procesos institucionales.

Este enfoque es consistente con estándares y referencias internacionales. Las Recomendaciones del Grupo de Acción Financiera Internacional (GAFI) —en particular la Recomendación 10, sobre debida diligencia del cliente, y la Recomendación 12, sobre Personas Expuestas Políticamente (PEP)— desarrollan el enfoque basado en riesgos para el conocimiento de contrapartes. Asimismo, la Convención de las Naciones Unidas contra la Corrupción (UNCAC) y las orientaciones de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en materia de integridad pública constituyen referentes para el fortalecimiento de mecanismos preventivos frente a los riesgos de corrupción en las relaciones del sector público.

La aplicación de estas orientaciones deberá considerar el marco normativo que resulte aplicable a cada entidad, de acuerdo con su naturaleza jurídica, funciones y nivel de exposición al riesgo. En este sentido, los estándares y referentes internacionales señalados constituyen criterios técnicos orientadores y no implican, por sí mismos, la creación de obligaciones adicionales a las previstas en el ordenamiento jurídico aplicable.

En consecuencia, la debida diligencia no debe entenderse únicamente como un requisito documental o contractual. Constituye un control preventivo que fortalece la capacidad institucional de las entidades distritales para gestionar los riesgos derivados de sus relaciones con terceros, proteger el patrimonio público y garantizar la transparencia en el uso de los recursos del Distrito Capital.

**Alcance del componente**

La debida diligencia se aplica a las relaciones institucionales y contrapartes que, de acuerdo con la naturaleza, funciones, procesos y contexto de cada entidad, puedan generar exposición a riesgos para la integridad pública. Para determinar su alcance, cada entidad deberá identificar y valorar las relaciones relevantes bajo un enfoque basado en riesgos, considerando, entre otros aspectos, las características de la relación, la contraparte involucrada, el nivel de exposición

identificado y las obligaciones que le resulten aplicables. Estas relaciones pueden comprender, de manera no taxativa:

- Contratos y convenios con personas naturales y jurídicas, incluyendo entidades sin ánimo de lucro y organizaciones de la sociedad civil.
- Acuerdos de cooperación nacional e internacional.
- Otorgamiento de subsidios, transferencias o beneficios económicos a terceros o a la ciudadanía.
- Licencias, permisos, autorizaciones o habilitaciones otorgadas a terceros, cuando por sus características y nivel de exposición al riesgo resulte pertinente aplicar medidas de debida diligencia.
- Relaciones con proveedores, contratistas e interventores en procesos de adquisición de bienes y servicios.
- Otras relaciones institucionales que, de acuerdo con el análisis realizado por la entidad, puedan generar una exposición relevante a riesgos para la integridad pública.

La identificación de una relación o contraparte dentro del alcance de la debida diligencia no implica la aplicación uniforme de las mismas medidas de conocimiento y verificación. Su naturaleza, alcance e intensidad deberán definirse de manera proporcional al nivel de riesgo identificado y de acuerdo con el marco normativo aplicable a cada entidad.

## 4.2. Debida diligencia como mecanismo preventivo en el marco del SIGRIP y el PTEP.

La debida diligencia corresponde al conjunto de medidas, procedimientos y controles orientados a conocer, verificar, analizar y monitorear las relaciones institucionales con terceros, con el fin de identificar y mitigar los riesgos que estas puedan representar para la integridad pública, el patrimonio de la entidad y la transparencia de la gestión. Más que un ejercicio de verificación documental se trata de un proceso activo de gestión del conocimiento sobre las contrapartes, que permite a la entidad actuar con diligencia razonable antes, durante y después de establecer una relación institucional.

En el contexto del SIGRIP, la debida diligencia opera como el principal mecanismo preventivo articulado con múltiples amenazas a la integridad pública. Su aplicación contribuye a la gestión de los riesgos asociados a LA/FT/FP, en la medida en que permite identificar señales de alerta asociadas a contrapartes con vínculos a actividades ilícitas. Pero también incide directamente en la prevención del soborno, el fraude y la corrupción, pues una entidad que conoce razonablemente con quién se relaciona está en mejor capacidad de detectar situaciones de riesgo antes de que estas se materialicen.

En las entidades distritales, la debida diligencia debe implementarse bajo un enfoque basado en riesgos. Esto implica que las medidas de verificación, monitoreo y control no deben aplicarse de manera uniforme a todas las relaciones institucionales, sino de forma diferenciada, proporcional y progresiva, según el nivel de exposición al riesgo que cada relación represente.

La implementación de este componente permite fortalecer la capacidad institucional para: conocer razonablemente las condiciones y características de las contrapartes; identificar señales

de alerta o factores de riesgo antes de iniciar o durante una relación institucional; documentar las verificaciones realizadas y las decisiones adoptadas; y monitorear continuamente las relaciones de mayor exposición al riesgo.

La debida diligencia se articula con los demás componentes del SIGRIP y debe concebirse como parte integral del ciclo de gestión del riesgo institucional. Su implementación eficaz depende de la actuación articulada de las tres líneas de aseguramiento: las áreas operativas que ejecutan los procesos con exposición al riesgo (primera línea), la función de cumplimiento que establece los criterios técnicos y analiza los casos de mayor complejidad (segunda línea), y la oficina de control interno que evalúa la eficacia del sistema (tercera línea).

La debida diligencia puede aplicarse en múltiples escenarios institucionales: la contratación pública, los convenios y alianzas, la cooperación nacional e internacional, la vinculación de organizaciones sociales en la ejecución de programas, y cualquier otra relación en la que la entidad ponga en juego sus recursos, su reputación o el bienestar de los ciudadanos que atiende. En este sentido, la debida diligencia debe articularse con otros componentes del SIGRIP, especialmente aquellos relacionados con la gestión de riesgos de corrupción, fraude, conflictos de interés y LA/FT/FP.

## 4.3. Tipos y aplicación de la debida diligencia

La aplicación de las medidas de debida diligencia debe responder a un enfoque basado en riesgos. El artículo 12 de la Ley 2195 de 2022 establece, entre otros criterios, la adopción de medidas razonables para verificar la información del beneficiario final y la realización de una debida diligencia continua que considere el perfil de riesgo de la contraparte. En concordancia con este marco, la Guía V7 del DAFP, así como las recomendaciones del GAFI y las orientaciones de la OCDE, aportan referentes técnicos para la aplicación gradual y proporcional de las medidas de debida diligencia, atendiendo el nivel de riesgo identificado.

Cuando resulte aplicable de acuerdo con la naturaleza de la contraparte y el marco normativo correspondiente, las medidas de debida diligencia incluirán la identificación del beneficiario final, entendido de conformidad con lo establecido en el artículo 631-5 del Estatuto Tributario y demás disposiciones aplicables. Su identificación y verificación se realizará atendiendo las características de la contraparte y bajo un enfoque basado en riesgos. Cuando se identifiquen factores de mayor exposición, podrán aplicarse medidas reforzadas para profundizar su conocimiento y verificación, de acuerdo con el marco normativo aplicable y el nivel de riesgo identificado.

Para efectos de la aplicación proporcional de la debida diligencia, se establecen tres niveles, de acuerdo con el perfil de riesgo de cada relación institucional:

**a. Debida diligencia simplificada**

La debida diligencia simplificada corresponde al conjunto mínimo de verificaciones orientadas a conocer razonablemente la identidad, existencia, actividad y propósito de la relación con una contraparte, cuando el perfil de riesgo de dicha relación sea bajo. Este nivel aplica a relaciones de bajo valor económico, corta duración, objeto específico y contrapartes con trayectoria conocida y antecedentes verificados.

Las verificaciones mínimas que componen este nivel incluyen:

- Verificación de identidad y existencia legal de la contraparte (persona natural o jurídica).
- Consulta de antecedentes disciplinarios ante la Procuraduría General de la Nación.
- Consulta de antecedentes fiscales ante la Contraloría General de la República.
- Consulta de antecedentes judiciales y del Registro Nacional de Medidas Correctivas (RNMC) de la Policía Nacional.
- Consulta del Registro de Deudores Alimentarios Morosos (REDAM), cuando corresponda según la naturaleza de la relación.
- Verificación de inhabilidades e incompatibilidades conforme a la normativa vigente.
- Verificación de existencia y representación legal ante cámara de comercio (para personas jurídicas).
- Consulta en las listas de designación de terroristas derivadas de resoluciones del Consejo de Seguridad de las Naciones Unidas incorporadas al ordenamiento colombiano.

**Ejemplo en contexto distrital:** Contratación de persona natural para prestación de servicios de apoyo administrativo por un período de meses. Se recomienda la debida diligencia simplificada ya que incluye la consulta de antecedentes y validación de identidad.

**b. Debida diligencia estándar**

La debida diligencia estándar incorpora medidas adicionales de validación y análisis para relaciones que presentan niveles intermedios de exposición al riesgo, mayor duración o cuando existan factores que ameriten mayor escrutinio sin alcanzar el umbral del nivel ampliado.

Además de las verificaciones del nivel simplificado, la debida diligencia estándar incorpora:

- Validación de información tributaria y del Registro Único Tributario (RUT).
- Verificación en el Registro Único de Proponentes (RUP), cuando aplique al proceso contractual.
- Revisión de fuentes abiertas y noticias reputacionales que puedan indicar situaciones de riesgo.
- Identificación básica de la estructura de propiedad o control de la persona jurídica, incluyendo representante legal y socios o accionistas mayoritarios.
- Consulta de fuentes internacionales complementarias de información, tales como las listas de sanciones administradas por la Oficina de Control de Activos Extranjeros de los Estados Unidos (OFAC) y la Unión Europea, así como información pública disponible de INTERPOL y la Administración para el Control de Drogas de los Estados Unidos (DEA), cuando resulte pertinente de acuerdo con la naturaleza de la relación y los riesgos identificados. Estas fuentes deberán utilizarse como insumo complementario para el análisis de riesgo, teniendo en cuenta su naturaleza, alcance y efectos jurídicos.

**Ejemplo en contexto distrital:** Convenio con una organización comunitaria para la ejecución de actividades de formación ciudadana, con recursos distritales. Se recomienda aplicar debida diligencia estándar, verificando adicionalmente la información reputacional de la organización y la identidad de sus representantes.

**c. Debida diligencia ampliada**

La debida diligencia ampliada corresponde a medidas intensificadas para relaciones de mayor exposición al riesgo. Este nivel es procedente cuando concurren factores que aumentan significativamente la probabilidad de que la relación institucional sea utilizada para actividades contrarias a la integridad pública. Conforme a las recomendaciones del GAFI (Recomendaciones 10 y 12) y la Guía V7 del DAFP de 2025, los factores que pueden activar este nivel incluyen, de manera enunciativa:

- La contraparte es una Persona Expuesta Políticamente (PEP) o tiene vínculos directos con PEPs, conforme a la definición del GAFI.
- La contraparte tiene domicilio, operaciones o vínculos en jurisdicciones de alto riesgo o bajo monitoreo reforzado según listas del GAFI o el GAFILAT.
- El contrato o convenio implica la transferencia de recursos significativos a zonas con presencia de grupos al margen de la ley o con alta incidencia de economías ilegales.
- La contraparte es de reciente creación, presenta estructura societaria compleja o hay dificultades para identificar a sus beneficiarios finales.
- Se han identificado previamente señales de alerta o situaciones inusuales en la relación con la contraparte.
- La naturaleza de la operación (objeto, monto, condiciones) se aparta significativamente de los patrones habituales de la entidad.

En estos casos, podrán aplicarse medidas adicionales, de acuerdo con los factores de riesgo identificados, tales como:

- Análisis detallado de la fuente de los recursos y la justificación económica de la relación.
- Profundización de la verificación del beneficiario final, cuando corresponda, mediante el análisis de la estructura de propiedad o control y la contrastación de la información disponible, de acuerdo con el nivel de riesgo identificado y el marco normativo aplicable.
- Verificación reforzada de información reputacional mediante múltiples fuentes públicas.
- Monitoreo intensificado durante la vigencia de la relación, con mayor frecuencia de seguimiento.
- Aprobación por parte de un nivel jerárquico superior antes de proceder con la relación.
- Documentación ampliada que sustente la decisión de iniciar o continuar la relación.

**Ejemplo en contexto distrital**:

Convenio con una organización no gubernamental internacional para la ejecución de un proyecto social en una localidad con presencia de grupos ilegales, por millones de pesos. Se aplica debida diligencia ampliada, incluyendo la profundización de la verificación del beneficiario final, el análisis de la estructura de la organización y un monitoreo reforzado durante la ejecución.

*Tabla 3 Criterios orientadores para la selección del nivel de debida diligencia*

| Factor | Simplificada | Estándar | Ampliada |
|---|---|---|---|
| **Valor del contrato** | Bajo (mínima cuantía o contratación directa) | Mediano (selección abreviada) | Alto o recursos significativos (licitación, convenios de gran cuantía) |
| **Trayectoria de la contraparte** | Conocida, con historial previo en la entidad | Conocida sin historial previo | Desconocida, nueva o con señales de alerta previas |
| **Perfil de la contraparte** | Sin factores de riesgo identificados | Estructura básica identificable | PEP, estructura compleja o jurisdicción de riesgo |
| **Zona de ejecución** | Sin factores de riesgo territorial | Presencia moderada de factores de riesgo | Alta incidencia de economías ilegales o grupos al margen de la ley |
| **Objeto del contrato** | Bienes o servicios estándar, objeto claro | Servicios especializados con beneficiarios identificados | Transferencias, atención a poblaciones vulnerables, zonas de riesgo |

Fuente: Elaboración propia con información normativa.

## 4.4. Implementación del componente de Debida Diligencia

La implementación de la debida diligencia requiere que las entidades adopten procedimientos claros que permitan integrar el conocimiento de las contrapartes a la gestión institucional del riesgo. En cada proceso en que la entidad establezca relaciones con terceros, deberán realizarse las verificaciones pertinentes conforme al nivel de riesgo identificado, documentando los resultados y articulando los hallazgos con los demás componentes del SIGRIP.

Como recomendación y para facilitar su comprensión y aplicación práctica a continuación, se presenta un proceso operativo en cinco pasos orientado a los líderes de proceso y servidores de las entidades distritales:

**PASO 1 ¿Qué relaciones debo someter a debida diligencia?**: Identifique las relaciones institucionales que involucran un flujo de recursos públicos, la habilitación de terceros para actuar en nombre de la entidad, o la ejecución de programas con impacto sobre la ciudadanía.

- Revise el mapa de procesos e identifique todas las actividades que implican contratación, convenios, subsidios, licencias o transferencias de recursos.
- Determine qué procesos tienen mayor exposición al riesgo por su valor, objeto, contraparte o zona de ejecución.
- Construya un inventario de relaciones institucionales susceptibles de generar exposición a riesgos de corrupción, soborno, fraude o LA/FT/FP.

**Pregunta clave:** *¿en qué momentos de la operación de mi entidad hay un vínculo entre recursos públicos y un tercero?*

**PASO 2 ¿Quién me preocupa? Segmentación y clasificación del riesgo:** Clasifique las contrapartes según su perfil de riesgo. No todas representan el mismo nivel de exposición.

- Agrupe las contrapartes según características comunes: tipo (natural o jurídica), antigüedad, sector, origen de recursos y zona de operación.
- Identifique si alguna contraparte es o tiene vínculos con una Persona Expuesta Políticamente (PEP), conforme a la Recomendación 12 del GAFI.
- Aplique el enfoque basado en riesgos: a mayor exposición, mayor intensidad de la verificación.
- Para la segmentación, considere variables como: tipo de contrato, cuantía, zona geográfica, objeto y condiciones de ejecución.

**Pregunta clave:** *¿qué sé realmente de con quién estoy operando?*

**PASO 3 ¿Qué verifico antes de iniciar la relación?:** La entidad deberá realizar las consultas correspondientes en las fuentes de información definidas de acuerdo con la naturaleza de la contraparte, el tipo de relación, el nivel de riesgo identificado y el marco normativo aplicable. Para estos efectos, se distinguirá entre fuentes de consulta obligatoria o con efectos vinculantes y fuentes complementarias de información y consulta:

**Fuentes de consulta obligatoria o con efectos vinculantes:** aquellas cuya consulta resulte obligatoria o cuyos resultados produzcan efectos jurídicos de acuerdo con el marco normativo aplicable. Entre estas podrán encontrarse, según corresponda, los antecedentes disciplinarios (Procuraduría), antecedentes fiscales (Contraloría), antecedentes judiciales, REDAM y RNMC, inhabilidades e incompatibilidades, existencia y representación legal (cámaras de comercio), RUP cuando aplique y las listas o fuentes relacionadas con designaciones de terrorismo que resulten vinculantes en Colombia de conformidad con el ordenamiento jurídico aplicable.

Cuando se identifique una coincidencia en alguna de estas fuentes, la entidad deberá actuar de conformidad con los efectos y obligaciones establecidos en las disposiciones aplicables.

**Fuentes complementarias de información y consulta:** de acuerdo con el nivel de riesgo y cuando resulte pertinente, podrán consultarse fuentes adicionales que contribuyan al conocimiento de la contraparte y a la identificación de señales de alerta. Entre ellas podrán considerarse las listas de sanciones administradas por la OFAC y la Unión Europea; la información pública disponible de INTERPOL y de la DEA; bases de datos reputacionales; fuentes abiertas y noticias; así como sistemas de alertas y herramientas de analítica.

Estas fuentes tienen distinta naturaleza, alcance y efectos jurídicos. Por esta razón, sus resultados deberán analizarse y contrastarse de acuerdo con el contexto de la relación y el nivel de riesgo identificado. Una coincidencia o señal de alerta encontrada en una fuente complementaria constituye un elemento para profundizar el análisis y, por sí sola, no genera automáticamente una consecuencia sobre la relación institucional, salvo que una disposición aplicable establezca lo contrario.

Las consultas se realizarán respecto de las personas naturales y, tratándose de personas jurídicas u otras estructuras, respecto de sus representantes y beneficiarios finales, cuando corresponda de acuerdo con la naturaleza de la contraparte, el nivel de riesgo identificado y el marco normativo aplicable.

**Pregunta clave:** *¿qué necesito verificar, y en qué profundidad, según el riesgo que representa esta contraparte?*

**PASO 4 ¿Qué hago durante la ejecución?:** La debida diligencia previa reduce el riesgo, no lo elimina. Mantenga un monitoreo activo durante la vigencia de la relación.

- Defina señales de alerta específicas para cada proceso con exposición al riesgo.
- Establezca la frecuencia del monitoreo según el nivel de riesgo: el monitoreo de relaciones con debida diligencia ampliada debe ser más frecuente.
- Actualice periódicamente la información de debida diligencia para relaciones recurrentes o de largo plazo.
- Preste atención a cambios en la estructura, representación, comportamiento o reputación de la contraparte que puedan indicar un riesgo sobrevenido.

**Pregunta clave:** *¿está ocurriendo algo que no corresponde al comportamiento esperado de esta contraparte?*

**PASO 5 ¿Qué hago si identifico una situación de riesgo?:** Cuando el proceso de debida diligencia revela señales de alerta, información inconsistente o inquietud razonable, la entidad debe actuar de manera estructurada. Detectar un riesgo no implica necesariamente suspender la relación, pero sí exige documentar, analizar y escalar adecuadamente.

- Si la señal tiene explicación razonable verificable: documente el análisis y mantenga monitoreo reforzado.
- Si no tiene explicación razonable: escale al responsable de la función de cumplimiento para análisis y decisión.
- Si se identifica una posible operación sospechosa relacionada con LA/FT/FP: active el procedimiento de Reporte de Operaciones Sospechosas (ROS) ante la UIAF, conforme al Capítulo 2 de este lineamiento.
- El servidor que identifica la señal no debe investigar por su cuenta ni confrontar directamente a la contraparte sobre sus sospechas (prohibición de tipping-off, artículo 105 del Estatuto Orgánico del Sistema Financiero).
- • Si la operación, vinculación o relación se realiza, seguir un proceso de integración y monitoreo de los riesgos identificados.
- Toda decisión debe quedar documentada con fecha, responsable, elementos analizados y conclusión.

**Pregunta clave:** *¿qué significa este hallazgo y qué hago con él?*

**Señales de alerta en la debida diligencia de contrapartes**

Las señales de alerta son situaciones que se apartan del comportamiento esperado de una contraparte y requieren mayor análisis. Las entidades distritales deben construir su propio catálogo adaptado a su contexto misional y al perfil de sus contrapartes habituales. A continuación, se presentan señales de referencia:

*Tabla 4 Señales de alerta en la debida diligencia de contrapartes*

| Categoría | Señales de alerta de referencia |
|---|---|
| **Identidad y existencia** | • Inconsistencias entre documentos aportados e información registrada en fuentes oficiales.<br>• Persona jurídica de reciente constitución que no guarda coherencia con la escala o complejidad del contrato al que aspira.<br>• Dificultad para identificar al representante legal o a los socios y accionistas reales.<br>• Nombre de la contraparte o sus representantes en listas vinculantes o restrictivas. |
| **Comportamiento y operación** | • Propuesta de condiciones contractuales inusuales: pagos anticipados desproporcionados o renuncia a garantías.<br>• Resistencia a suministrar información requerida para el proceso de debida diligencia o el seguimiento de la ejecución.<br>• Cambios súbitos en la representación legal o en la estructura de la entidad durante la ejecución del contrato.<br>• Facturación de bienes o servicios que no corresponden a la ejecución verificada en campo. |
| **Reputación e información pública** | • Noticias o reportes que vinculen a la contraparte o sus representantes con corrupción, lavado de activos u otras conductas ilícitas.<br>• Antecedentes disciplinarios o fiscales no declarados o incompatibles con la contratación.<br>• Vinculaciones conocidas con personas o entidades sancionadas por autoridades nacionales o internacionales. |

Fuente: Elaboración propia con recomendaciones para el lineamiento.

La conservación documental del proceso de debida diligencia es necesaria para garantizar la trazabilidad de las verificaciones realizadas, las decisiones adoptadas y la disponibilidad de la información ante las autoridades competentes. Para los sujetos obligados en los términos del artículo 12 de la Ley 2195 de 2022, la información obtenida en aplicación del principio de debida diligencia deberá conservarse durante el tiempo que dure el negocio jurídico o el contrato estatal y, al menos, durante los cinco (5) años siguientes, contados a partir del 1.º de enero del año siguiente a aquel en que se dé por terminado el negocio jurídico o el contrato estatal o se efectúe la transacción ocasional. Lo anterior deberá articularse con las disposiciones aplicables en materia de gestión documental y los instrumentos archivísticos de cada entidad.

## 4.5. Construcción del Manual de Debida Diligencia

De acuerdo con la Guía para la Administración del Riesgo Versión 7 del DAFP, las entidades deben contar con un Manual de Debida Diligencia articulado con el SIGRIP y el PTEP. Este manual es el instrumento operativo central del componente: define qué verificaciones se realizan, cuándo, quién las realiza, cómo se documentan los resultados y qué se hace con los hallazgos.

La construcción del manual debe orientarse bajo un enfoque basado en riesgos, evitando cargas documentales innecesarias. Para las entidades que están iniciando la implementación del componente, es válido comenzar con un manual básico que cubra los elementos mínimos e irlo ampliando progresivamente conforme se fortalezcan las capacidades institucionales.

El Manual de Debida Diligencia deberá contener, como mínimo, los siguientes elementos:

*Tabla 5 Elementos mínimos del manual de Debida Diligencia*

| Elemento del Manual | Contenido mínimo requerido |
|---|---|
| **1. Alcance del componente** | Definición de las relaciones institucionales a las que aplica la debida diligencia, indicando los procesos y tipos de contrapartes cubiertos. |
| **2. Marco normativo y conceptual** | Disposiciones que sustentan el componente, incluyendo las normas del PTEP, el SIGRIP y la gestión del riesgo aplicables a la entidad. |
| **3. Roles y responsabilidades** | Qué dependencias participan, cuáles son sus responsabilidades y cómo se articulan con la función de cumplimiento y el control interno. |
| **4. Criterios de segmentación y clasificación del riesgo** | Variables e indicadores que determinan el nivel de debida diligencia (simplificada, estándar o ampliada) según el perfil de riesgo de la contraparte y la operación. |
| **5. Procedimiento operativo** | Etapas del proceso: identificación de la relación, recolección de información, análisis y valoración, decisión, documentación y conservación. |
| **6. Mecanismos de consulta y verificación** | Fuentes de información a consultar, diferenciando entre las de uso obligatorio (vinculantes) y las de uso proporcional al riesgo (complementarias), con indicación del responsable de cada consulta. |
| **7. Monitoreo y actualización periódica** | Cuando se actualiza la información de debida diligencia, especialmente para relaciones recurrentes o de largo plazo. Incluye frecuencia, responsable y criterios de activación del monitoreo intensificado. |
| **8. Criterios de escalamiento y toma de decisiones** | Qué casos requieren aprobación de niveles superiores, cuándo se activa la función de cumplimiento y cuándo se suspende o termina una relación por razones de riesgo. |
| **9. Conservación documental y trazabilidad** | Responsables, tiempos de conservación, mecanismos de almacenamiento y criterios de acceso a la información, articulados con la gestión documental institucional. |

| Elemento del Manual | Contenido mínimo requerido |
|---|---|
| **10. Mejora continua** | Procesos de evaluación periódica, seguimiento de hallazgos, revisión de incidentes, fortalecimiento de señales de alerta y actualización de criterios de riesgo basados en la experiencia institucional. |

**Fuente:** Elaboración propia para el documento de lineamientos.

# Capítulo 5 Canales de Denuncia

## 5.1. Contexto normativo y conceptual

El Observatorio Distrital de Contratación y Lucha Anticorrupción - ODCLA señala que la denuncia implica el ejercicio de un deber jurídico, establecido en la Constitución Política de Colombia (Art. 95.7 CP), del cual es titular la persona o el servidor público que tuviere conocimiento de la comisión de un posible delito que deba investigarse de oficio (Observatorio Distrital de Contratación y Lucha Anticorrupción, 2024). En este contexto, las denuncias tienen un carácter informativo al poner en conocimiento de la autoridad encargada de investigar, la perpetración de una conducta presumiblemente delictuosa, con indicación de las circunstancias de tiempo, modo y lugar en que se realizó y de los presuntos autores o partícipes, si fueren conocidos por el denunciante (Observatorio Distrital de Contratación y Lucha Anticorrupción, 2024).

El artículo 31 de la ley 2195 de 2022, modificó el artículo 73 de la Ley 1474 de 2011, estableció la formulación de un componente sobre canales de denuncia dentro de los PTEP, siguiendo lo señalado en el artículo 76 de la Ley 1474 de 2011, donde se menciona que todas las entidades públicas deberán disponer de un espacio en su página web para que *los ciudadanos presenten quejas y denuncias de los actos de corrupción realizados por funcionarios de la entidad*, y de los cuales tengan conocimiento. Por lo cual, la *oficina de quejas, sugerencias y reclamos será la encargada de conocer dichas quejas para realizar la investigación correspondiente en coordinación con el operador disciplinario interno,* con el fin de iniciar las investigaciones a que hubiere lugar. (Congreso de Colombia, 2011)

Así, las entidades públicas en el PTEP deberán definir acciones que permitan estructurar la recepción de denuncias para la detección temprana de posibles afectaciones a la integridad, garantizar un tratamiento adecuado y oportuno de los reportes recibidos y proteger a quienes denuncian frente a riesgos de represalia (Secretaría General, 2026). Así mismo, cuando la denuncia cuente con suficientes evidencias, se deberán adelantar las investigaciones correspondientes por parte del operador disciplinario interno, teniendo en cuenta lo mencionado en el artículo 94 de la Ley 1952 de 2019, donde se señala que toda entidad u organismo del Estado *debe organizar una unidad u oficina del más alto nivel encargada de conocer los procesos disciplinarios que se adelanten contra sus servidores.* Si no fuere posible garantizar la segunda instancia por razones de estructura organizacional, *esta será de competencia de la Procuraduría General de la Nación de acuerdo con sus competencias.* (Congreso de Colombia , 2019)

### 5.1.1 Elementos para la gestión de denuncias

Según define la Guía para la Gestión Integral del Riesgo en Entidades Públicas, el Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP, permite prevenir, detectar y corregir los eventos que amenazan el ejercicio íntegro del servicio público o la integridad de las instituciones del Estado de manera integral (Departamento Administrativo de la Función Pública, 2025). Allí, la atención de denuncias se presenta como una herramienta que contribuye en la gestión de riesgos. Por lo cual, se establece que las entidades deberán formular un procedimiento interno que, contenga:

- Los medios de recepción de denuncias e inquietudes.
- El paso a paso para evaluar las denuncias e inquietudes que se presenten por el canal.
- El paso a paso para tratar las denuncias e inquietudes que correspondan al canal.
- El paso a paso para concluir el trámite de las denuncias e inquietudes, de conformidad con el tratamiento realizado. (Departamento Administrativo de la Función Pública, 2025)

A nivel Distrital, la gestión de denuncias está orientada por la Directiva Conjunta 005 de 2023, que definen la operación de los canales de denuncia bajo criterios de trazabilidad, oportunidad, confidencialidad y reserva, y proporciona elementos para la recepción, análisis, seguimiento y cierre de las denuncias (Secretaría General, 2026). En particular, la Directiva Conjunta 005 establece las directrices para la atención y gestión de denuncias presentadas por la ciudadanía, a partir de:

- Armonización y centralización de canales para la recepción de denuncias, a través de Bogotá Te Escucha.
- Registro de denuncias elevadas por la ciudadanía a través de los diferentes canales de atención.
- Aspectos a tener en cuenta por parte de las Oficinas de Control Disciplinario Interno frente a las denuncias por posibles actos de corrupción.
- Medidas para la protección de identidad del o la denunciante.
- Difusión de las directrices y reporte mensual de las denuncias que ingresan a través del Sistema Distrital para la Gestión de Peticiones Ciudadanas - “Bogotá te escucha”.

Por lo cual, se cuenta con una serie de antecedentes para estructurar la gestión de denuncias dentro del SIGRIP, y a partir de allí, identificar en qué nivel de madurez se encuentran las entidades distritales para robustecer sus acciones y la operación de los canales de recepción, a través del PTEP.

A su vez, el Decreto 479 de 2024 “por medio del cual se adopta el Modelo de Gestión Jurídica Anticorrupción para el Distrito Capital y se dictan otras disposiciones”, en el título IV definió el protocolo para la recepción de denuncias, como herramienta anticorrupción del Modelo. El artículo 340 y 342 menciona que las entidades y organismos distritales fortalecerán la difusión y operación de los canales de recepción de denuncias, a partir de:

- Claridad sobre su disponibilidad, ubicación y especialidad, además de la gestión y seguimiento de estas.

- En caso de que las denuncias no presenten evidencias o motivos razonables para adelantar una actuación, se deberá considerar como *alerta* para establecer las acciones de carácter general que se consideren pertinentes aplicar.
- Medidas de protección de identidad del denunciante, cuando la información suministrada pueda poner en riesgo a la integridad del denunciante, se habilitará en el canal un espacio para que las personas manifiesten la necesidad de contar con una medida de protección.
- Las medidas de protección buscan, además, incentivar la entrega de información, queja, denuncia o testimonio sobre actos susceptibles de ser investigados y sancionados en el ámbito fiscal, disciplinario o penal, por actos de corrupción. (Alcaldía Mayor de Bogotá, 2022)

Así mismo, el Modelo de Gestión Jurídica Anticorrupción señala tener en cuenta las directrices desarrolladas en la Directiva Conjunta 005 de 2023, previamente señaladas.

## 5.2. Recomendaciones para la elaboración del procedimiento para la operación del canal institucional de denuncias por corrupción.

A continuación, se presentarán algunas orientaciones para la formulación del procedimiento para la atención de denuncias externas en las entidades distritales, teniendo en cuenta que los lineamientos vigentes para esta temática están centrados en la gestión de los reportes que realiza la ciudadanía. De esta manera, este procedimiento es una herramienta que contribuye en la gestión de riesgos dentro del SIGRIP y permite la coordinación de esfuerzos institucionales para la adecuada gestión de las denuncias, así se presentan las siguientes recomendaciones para su elaboración:

**a. Planeación del procedimiento**

- Definir el objetivo que orientará la gestión de denuncias en la entidad, teniendo presente su funcionalidad en la gestión de riesgos. Al igual que definir las áreas y dependencias que participan en la recepción, análisis y gestión de las denuncias.

- Presentar las definiciones y terminología que constituyen la gestión de denuncias, y los lineamientos, normas o políticas que dan sustento a esta gestión.

- Desarrollar las actividades que conforman la atención de denuncias, presentando una descripción sobre sus características, responsables, evidencias o registros asociados, tiempos y puntos de control. En estas actividades se deberá identificar:

I. Los medios o canales habilitados para la recepción de denuncias, en articulación con el sistema Distrital Bogotá Te Escucha.
II. Los criterios para evaluar las denuncias e identificar si corresponden con un posible hecho de corrupción.
III. La ruta para gestionar las denuncias que correspondan con posibles hechos de corrupción.
IV. Las herramientas para promover medidas de protección al denunciante y enfoques diferenciales.
V. Los mecanismos para la sistematización, seguimiento y monitoreo sobre las denuncias y la articulación con SIGRIP, como posibles alertas para la gestión institucional.

Este procedimiento deberá estar armonizado con la gestión de PQRS que realiza la entidad, en cuanto a los tiempos de respuesta y responsables, y deberá surtir el flujo de aprobación definido en la entidad, según el Sistema de Gestión de Calidad.

**b. Implementación y difusión del procedimiento**

Una vez aprobado el procedimiento diseñado, se sugiere implementar su contenido a partir de la operación del canal definido, la recepción, análisis, gestión y respuesta a las denuncias recibidas en la entidad. En caso de identificar denuncias reiterativas con suficiente material probatorio o evidencias de irregularidades, se sugiere tomar correctivos efectivos orientados al desarrollo de las investigaciones disciplinarias a las que haya lugar, implementar ajustes a los procesos o procedimientos y acciones de mejora, con el fin de retroalimentar la gestión institucional a partir de las denuncias recibidas.

Así mismo, se recomienda implementar acciones para la difusión del procedimiento a nivel interno y externo en la entidad, con el fin de favorecer la apropiación de su contenido por parte de los servidores y contratistas, y orientar a la ciudadanía sobre cómo presentar denuncias e identificar situaciones que realmente correspondan a hechos de corrupción administrativa.

**c. Seguimiento, evaluación y mejora continua del procedimiento**

Se sugiere realizar un seguimiento periódico interno y externo, que permita identificar la efectividad del procedimiento diseñado, y su relevancia en la gestión de denuncias. Dentro del componente interno, se sugiere consolidar reportes institucionales sobre el número de denuncias recibidas y atendidas, tiempos de respuesta, agrupación por tipologías o temáticas, y acciones de mejora implementadas.

A nivel externo, se recomienda implementar instrumentos que permitan conocer la experiencia ciudadana en la interposición de denuncias, a fin de identificar la efectividad del procedimiento y los niveles de confianza en el mismo.

Con estos insumos, se sugiere actualizar o ajustar el procedimiento diseñado, incluir los principales hallazgos de la gestión de denuncias dentro de la gestión de riesgos, fortalecer analítica y tableros de control sobre las denuncias, diseñar acciones preventivas y sistematizar y compartir buenas prácticas.

# Bibliografía


Alcaldía Mayor de Bogotá. (2022). *Decreto 610 de 2022.* Bogotá.

Colombia. Congreso de la República . (2000). *Ley 599 de 2000, arts 25,323 y 345.*

Colombia. Congreso de la República . (2022). *Ley 2195 .*

Colombia. Congreso de la República. (1999). *Ley 526, art.9 .*

Colombia. Congreso de la República. (2006). *Ley 1121 de 2006, art. 27.*

Colombia. Congreso de la República. (2008). *Ley 1186 de 2008.*

Colombia. Congreso de la República. (2008). *Ley 1186 de 2008.*

Colombia. Congreso de la República. (2024). *Decreto 1122 .*

Colombia. Presidencia de la República. (2002). *Decreto 1497 de 2002.*

Concejo de Bogotá, D. C. (2026). *Acuerdo Distrital 1025 de 2026, por medio del cual se establecen lineamientos para el seguimiento y verificación de la adopción de mecanismos de prevención y control del riesgo de lavado de activos y financiación del terrorismo por parte de las entidades .* Bogotá D.C.: Febrero.

Congreso de Colombia . (2019). *Ley 1952 de 2019*. Obtenido de Gestor Normativo : https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=90324

Congreso de Colombia. (2011). *Ley 1474 de 2011*. Obtenido de Gestor Normativo: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=43292

Congreso de la República de Colombia. (1995). *LEY 190 .* Diario Oficial No. 43.654.

Congreso de la República de Colombia. (1999). *Ley 526 de 1999.*

Congreso de la República de Colombia. (1993). *Ley 67 de 1993, por medio de la cual se aprueba la Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas.*

Congreso de la República de Colombia. (2003). *Ley 800 de 2003, por medio de la cual se aprueba la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.*

Congreso de la República de Colombia. (2003). *Ley 808 de 2003, por medio de la cual se aprueba el Convenio Internacional para la Represión de la Financiación del Terrorismo.*

Consejo Distrital de Política Económica y Social del Distrito Capital. (CONPES D.C.). (2019). *Documento CONPES D.C. 01: Política Pública Distrital de Transparencia, Integridad y No Tolerancia con la Corrupción.* Bogotá, D. C.

Consejo Nacional de Política Económica y Social (CONPES). (2021). *Documento CONPES 4042: Política Nacional Antilavado de Activos, Contra la Financiación del Terrorismo y*

*Contra la Financiación de la Proliferación de Armas de Destrucción Masiva.* Bogotá, D. C.

Departamento Administrativo de la Función Pública. (2025). *Guía para la Gestión Integral del Riesgo en Entidades Públicas.* Bogotá.

Departamento Administrativo del Servicio Civil Distrital. (2021). *Concepto 2021EE956. Respuesta al radicado 2021ER728 sobre la utilización del término colaboradores en la administración pública.* Bogotá D.C.

Departamento Nacional de Planeación (DNP). (2021). *CONPES 4042 de 2021.*

Grupo de Acción Financiera de Latinoamérica (GAFILAT). (s.f.). *¿Qué es el GAFILAT?* Obtenido de GAFILAT: https://www.gafilat.org/index.php/es/gafilat/que-es-gafilat

Grupo de Acción Financiera Internacional (GAFI). (2012). *Recomendaciones del GAFI.*

Grupo de Acción Financiera Internacional (GAFI). (2012, actualizado en 2026). *Estándares internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación: Las Recomendaciones del GAFI.* Obtenido de https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

Naciones Unidas. (1988). *Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas.*

Naciones Unidas. (1999). *Convenio Internacional para la Represión de la Financiación del Terrorismo.*

Naciones Unidas. (2000). *Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.*

Observatorio Distrital de Contratación y Lucha Anticorrupción. (2024). *Denuncia efectiva y protección al denunciante en el marco de la lucha contra la corrupción administrativa en el Distrito Capital.* Bogotá: Secretaría Jurídica Distritral.

Organización de las Naciones Unidas (ONU). (s.f.). *Resoluciones del Consejo de Seguridad.*

Secretaría General. (2026). *Lineamientos técnicos distritrales para la implementación de los Programas de Transparencia y Ética Pública - PTEP.* Bogotá: Alcaldía Mayor de Bogotá.

Secretaría General de la Alcadía Mayor de Bogotá D.C. (2022). *Documento Técnico de Adaptación Medidas de Prevención y Mitigacion - SARLAFT.*

Secretaria General de la Alcaldía Mayor de Bogotá D.C. . (2021). *Ruta Metodológica SARLAFT.*

Secretaría General de la Alcaldía Mayor de Bogotá D.C. (2020). *Circular 092 .*

Secretaría Juridica Distrital. (2026). *Operación del Sistema Integral de Gestión de Riesgos para la Integridad Pública (SIGRIP)*. Obtenido de https://secretariajuridica.gov.co/node/5227

Superintendencia Financiera de Colombia. (2020). *Circular Externa 027 de 2020. Instrucciones relativas a la administración del riesgo de lavado de activos y de la financiación del terrorismo (SARLAFT).* Obtenido de

https://www.superfinanciera.gov.co/publicaciones/10102740/normativanormativa-generalcirculares-externas-cartas-circulares-y-resoluciones-desde-el-ano-circulares-externascirculares-externas-10102740/

Unidad de Análisis Financiero - UIAF. (Octubre de 2025). *Documento técnio e instructivo para el reporte de operaciones sospechosas de las entidades obligadas a reportar bao la Ley 2195 de 2022: Anexo 1.*

Unidad de Información y Análisis Financiero - UIAF. (14 de Enero de 2020). *Guía de buenas prácticas del ROS.* Obtenido de https://www.uiaf.gov.co/publicaciones

Unidad de Información y Análisis Financiero (UIAF). (2014). *Lo que debe saber sobre el lavado de activos y la financiación del terrorismo (p. 33).*

Unidad de Información y Análisis Financiero (UIAF). (s.f.). *Documento de preguntas frecuentes.* Obtenido de https://www.uiaf.gov.co/node/1272

Unidad de Información y Análisis Financiero (UIAF). (s.f.). *Grupo de Acción Financiera Internacional (GAFI).* Obtenido de Unidad de Información y Análisis Financiero.: https://www.uiaf.gov.co/grupo-de-accion-financiera-internacional-gafi

Unidad de Información y Análisis Financiero. (2022). *Manual de usuario del Sistema de Reporte en Línea (SIREL).* Obtenido de https://www.uiaf.gov.co/sites/default/files/inline-images/Manual%20de%20usuario%20SIREL2022%20%284%29.pdf